Hindawi
Security and Communication Networks
Volume 2021, Article ID 4939589, 11 pages
https://doi.org/10.1155/2021/4939589

Research Article

A Lightweight and Secure Anonymous User Authentication Protocol for Wireless Body Area Networks

Junsong Zhang,[1] **Qikun Zhang**,[1] **Zhigang Li**,[1] **Xianling Lu**,[2] **and Yong Gan**[3]

[1]*School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China*
[2]*School of Information Engineering, Zhengzhou University of Industrial Technology, Zhengzhou 450002, China*
[3]*School of Information Engineering, Zhengzhou University of Technology, Zhengzhou 450002, China*

Correspondence should be addressed to Xianling Lu; 2014102@zzuli.edu.cn

Received 19 May 2021; Accepted 6 July 2021; Published 22 July 2021

Academic Editor: Jie Cui

The recent development of wireless body area network (WBAN) technology plays a significant role in the modern healthcare system for patient health monitoring. However, owing to the open nature of the wireless channel and the sensitivity of the transmitted messages, the data security and privacy threats in WBAN have been widely discussed and must be solved. In recent years, many authentication protocols had been proposed to provide security and privacy protection in WBANs. However, many of these schemes are not computationally efficient in the authentication process. Inspired by these studies, a lightweight and secure anonymous authentication protocol is presented to provide data security and privacy for WBANs. The proposed scheme adopts a random value and hash function to provide user anonymity. Besides, the proposed protocol can provide user authentication without a trusted third party, which makes the proposed scheme have no computational bottleneck in terms of architecture. Finally, the security and performance analyses demonstrate that the proposed scheme can meet security requirements with low computational and communication costs.

1. Introduction

In recent years, along with the quick development of communications and microelectronics technologies, a new network paradigm for detecting human body data, named wireless body area networks (WBANs) [1], has emerged. A typical architecture of WBAN for the healthcare system is depicted in Figure 1. There are three main participants in the WBAN: a dynamic set of M patients with monitoring sensors, denoted as PAT $= \{P_j | j = 1, 2, \ldots, M\}$, a set of N doctors as DCT$\{D_i | i = 1, 2, \ldots, N\}$, and a registration center (RC) as a trusted third party [2]. The sensors are mainly embedded or worn on the patient. Their main function is to collect various physical parameters of the patient, such as blood pressure (BP), electrocardiogram (ECG), and temperature, and then transmit these data to the personal terminal. Next, the personal terminal uses a wireless communication technology (such as Wi-Fi and 4G/5G/CDMA) to forward all collected information to the appropriate doctor or the medical server. Therefore, the personal terminal acts as a bridge between the doctors and WBAN. These sensory data collected from the patient will play an important role in the doctor's medical diagnosis. In addition, this new technology not only helps to monitor and improve the health of patients but is also more suitable for health monitoring and care for the elderly and the disabled. However, due to the openness of the wireless channel, the data transmitted in WBAN can easily be eavesdropped or tampered with by unauthorized users. Since these sensitive patient data are the basis of clinical diagnosis, any data leakage or modification may put the patient's life at risk [3–5]. Consequently, it is necessary and important to provide a safe and reliable authentication protocol in the WBAN to ensure that only legitimate users can obtain the patient's sensitive information.

Since the collected information is vital to the patient's life, it is very confidential and vulnerable to various attacks by an adversary. If these sensitive data are obtained and

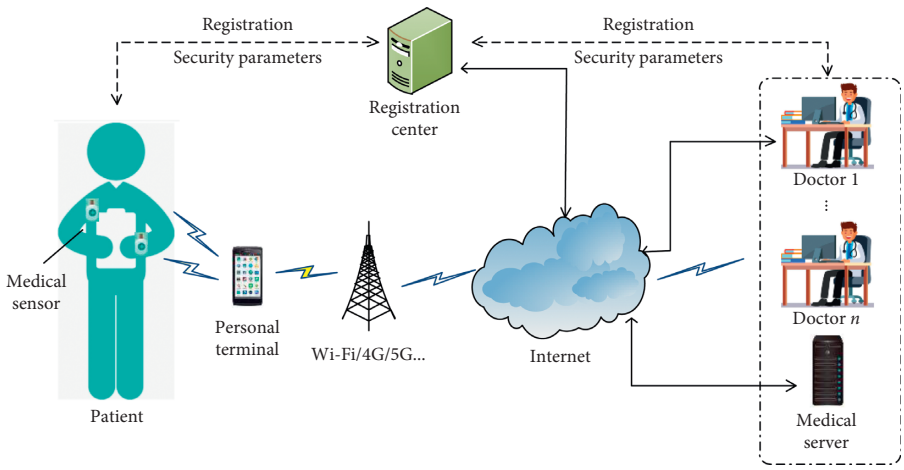

Figure 1: A typical system model of the WBAN.

misused by an adversary, it may threaten the lives of patients. Therefore, it is important to provide data security and privacy protection to the WBAN [6]. In other words, strong security solutions and authentication protocols are necessary for the success and large-scale deployment of the WBANs. Motivated by these shortcomings, we proposed a lightweight and secure anonymous user authentication protocol for the WBAN. The contributions of the paper are summarized as follows:

(1) To guarantee the privacy of doctors and patients in the WBAN, an efficient ECC-based privacy-preserving authentication is proposed. Moreover, the proposed authentication protocol can verify the legitimacy of the patients and doctors.

(2) In the proposed authentication protocol, under the premise of anonymous authentication of users, no trusted third party is required to participate in the authentication process. In this way, the proposed authentication protocol has no computational bottleneck in terms of architecture. Besides, the proposed scheme can provide a low computation burden on the client side, which makes the proposed authentication protocol more efficient.

(3) The proposed authentication protocol provides a method for RC to track the doctor's actual identity. At the same time, it also ensures that the doctor's identity information is not obtained by unrelated parties. This makes it possible to prevent doctors from making a wrong diagnosis or to pursue accountability afterward.

(4) A detailed security analysis and performance analysis show that the proposed authentication protocol can meet the security and performance requirements of the WBAN application.

The rest of the paper is organized as follows. Section 2 discusses the existing secure authentication schemes. Section 3 describes the attacker models and preliminaries. Section 4 presents the proposed mutual authentication scheme. Security and performance analyses of the proposed protocol are provided in Sections 5 and 6, respectively. Finally, Section 7 gives the conclusion of this paper.

2. Related Work

Security, privacy, and identity authentication are the most critical and challenging issues in the WBAN. During the last few years, so many authentication protocols have been proposed to solve the security and privacy protection problem for wireless-based healthcare applications [7–10]. Some research activities use public key cryptography (PKC) to build authentication schemes [7, 8]. Since the traditional PKC requires a large amount of computation overhead, these existing PKC-based methods are not suitable for the resource-constrained WBAN. In 2014, Chatterjee et al. [9] presented an ECC-based user authentication for WBAN. Liu et al. [10] proposed a lightweight certificateless authentication scheme that uses ECC and bilinear pairings. Unfortunately, their method was found to be unable to resist tracking attack and impersonation attack [11].

In 2015, Das et al. [12] suggested a biometric-based authentication protocol for WBAN. Their proposed protocol combines biometric information and a password to verify the legitimacy of the user. Later, Wang and Zhang [13] found that Das et al.'s scheme is not able to provide user anonymity. In order to avoid this defect, they proposed a new bilinear pairing-based authentication protocol in the WBAN environment. In the same year, Debiao et al. [14] presented a bilinear pairing-based anonymous authentication scheme for WBAN. Liu et al. [15] proposed an anonymous 1-round authentication protocol for WBANs. They claimed that their authentication scheme was efficient and secure. However, Li et al. [16] demonstrated that Liu et al.'s scheme is unable to resist impersonation attack, DoS attack, and session key guessing attack. To avoid these flaws, they proposed an improved 1-round authentication protocol for WBANs. Later, Shen et al. [17] presented a lightweight nonpairing certificateless authentication protocol for WBANs. Unfortunately, their proposed scheme was found to be unable to resist the impersonation attack. To remove the flaws, Liu

et al. [18] proposed an improved authentication to remedy the flaws in Shen et al.'s scheme. Wazid et al. [19] proposed a novel authentication and key management scheme for the cloud-assisted WBAN.

Later, Qiu et al. [20] proposed a secure mutual authentication protocol based on ECC for wireless medical sensor networks. In this paper, the BAN logic is used to prove the security of the proposed scheme. However, according to [21], it is still suffering from insider attack. Shen et al. [21] presented a cloud-aided certificateless and privacy-preserving authentication scheme for the WBAN. In [21], the authors use public key cryptography and the message authentication code (MAC) to achieve user authentication. Shuai et al. [22] presented a bilinear pairing-based mutual authentication scheme for WBAN. Fotouhi et al. [23] propose a new lightweight hash chain-based and forward secure authentication scheme for WBAN. Kumar et al. [24] presented an ECC-based authentication scheme for wearable devices environment. Jegadeesan et al. [25] proposed an efficient privacy-preserving anonymous authentication for WBAN. However, their scheme is also not able to resist the impersonation attack.

To enhance the security of WBAN, a novel lightweight and secure anonymous user authentication protocol was designed. Compared with other existing schemes, the scheme proposed in this paper has two distinct characteristics. First, the proposed scheme does not require a trusted third party to verify the legitimacy of users anonymously. Second, the proposed authentication protocol provides a method for RC to track the doctor's actual identity, which can reduce the doctor's misbehaving.

3. Preliminaries

3.1. Threat Model. An adversary model is a valid abstraction of an arbitrary adversary which is able to lunch a successful attack. Due to the open nature of WBAN, the wireless communication channel is vulnerable to various attacks. In the proposed authentication protocol, the two widely used models, named Dolev–Yao model and CK-adversary model, are used. In the Dolev–Yao model, the communication between different entities can be intercepted by an adversary. Besides, the adversary is also able to modify/delete/fake/inject into the transmitting information [26, 27]. In the CK-adversary model, the adversary can control all the communication between the entities. Moreover, the adversary is assumed to be able to extract the secret parameters stored in the entity's memory and the temporary data used to establish session keys [6]. Furthermore, the adversary can use oracle queries to interact with the entities. As far as we know, these two adversary models are widely adopted in the authenticated key exchange protocols [28].

3.2. Security Requirements for the WBAN. The communication of the WBAN is mainly divided into two types: the communication between the sensor and the personal terminal and the communication between the personal terminal and the back-end server. Our work focuses on the security of communication between the personal terminal and the back-end server. In this section, we discuss the security and privacy requirements for the WBAN environment [29].

3.2.1. Mutual Authentication. As we all know, the messages transmitted in the WBAN are easily eavesdropped and modified. Hence, once a message is received, the most important thing for the receiver is to determine whether the message is sent by a legitimate user and whether the message has been modified. Therefore, there should be a mechanism to verify the legitimacy of the message and the sender of the message.

3.2.2. Data Integrity. To ensure the integrity of the transmitted message in the WBAN, an anonymous signature mechanism is attached to the transmitted message.

3.2.3. Confidentiality. Since the messages transmitted in the WBAN contain the patient's sensitive information, and this sensitive information is very important privacy for patients. Therefore, the proposed protocol needs to ensure that the unauthorized entities cannot obtain the content of the transmitted message.

3.2.4. Identity Privacy-Preserving. To protect the identity privacy of users (especially the patients), the actual identity of the patients cannot directly appear in the transmitted messages. Besides, the proposed protocol also needs to ensure that the adversary cannot decipher/calculate the patient's actual identity through the message.

3.2.5. Conditional Traceability. In WBAN, for the manager, the doctor's identity should be traceable. Especially when a doctor makes any dispute or misbehavior, the manager needs to have the ability to get the doctor's actual identity. This provides a basis for subsequent accountability and can also reduce the loss of WBAN.

3.2.6. Attack Resistance. To ensure secure communication in WBANs, the proposed protocol should be able to withstand various common attacks, such as replay attack, impersonation attack, and man-in-the-middle attack.

3.3. Elliptic Curve Cryptography. Elliptic curve cryptography (ECC) is one of the most widely used public key asymmetric cryptographies [30]. Its security comes from the discrete logarithm problem (DLP) in a group defined by points on elliptic curve. An elliptic curve E over $GF(p)$, where p is a large prime, is defined by an equation of the following form:

$$y^2 = x^3 + ax + b, \tag{1}$$

where $a, b \in GF(p)$ and satisfies $4a^3 + 27b^2 \neq 0 \pmod{p}$. There are two basic operations on ECC: point addition and

scalar multiplication. The scalar multiplication over E can be computed by repeated addition as

$$k \cdot P = P + P + \cdots + P\,(k \text{ times}). \tag{2}$$

The hardness of the elliptic curve discrete logarithm problem is essential for the security of all elliptic curve cryptographic schemes. Here, we present two important mathematical problems on elliptic curves as follows [31]:

Elliptic curve discrete logarithm problem (ECDLP): given an elliptic curve E defined over a finite field $GF(p)$, and two points $Q, P \in E$ of order q, it is hard to find an integer $k \in Z^*q$ such that $Q = k \cdot P$

Elliptic curve Diffie–Hellman problem (ECDHP): given an elliptic curve E defined over a finite field $GF(p)$, a point $P \in E$ of order n, $A = aP$, $B = bP$, and find the point $C = abP$

4. The Proposed Authentication Protocol

In this section, we present our proposed authentication protocol for WBAN. The proposed protocol consists of three phases: system initialization, registration, and anonymous mutual authentication. All the notations used in this paper are presented in Table 1. The detailed descriptions of these phases are explained as follows.

4.1. System Initialization. In the proposed authentication protocol, as mentioned earlier, RC is considered as a trusted third party. It is responsible for the registration of all patients and doctors in the WBAN. At the same time, it must also set relevant security parameters for the authentication protocol.

Step I-1: RC selects an appropriate elliptic curve E over the finite field $GF(p)$. Then, RC chooses a bilinear mapping $\hat{e}$: $G_1 \times G_1 \longrightarrow G_2$ and the generator $P_0 \in G_1$ with the order q over elliptic curve E, where q is a big prime number.

Step I-2: RC chooses two secure hash function h and H, where h:$\{0, 1\}^* \longrightarrow Z^*q$, H: $\{P \in E\} \longrightarrow \{0, 1\}^l$, in which l is the length of the string. Next, RC selects two random number $u, v \in Z^*q$ as secret values and keeps them properly.

Step I-3: RC chooses a random number s_{RC} as its master key and computes the corresponding public key $PK_{\mathrm{RC}} = s_{\mathrm{RC}} \cdot P$. Then, RC publishes the public system parameters to the users: $param = \{E, G_1, G_T, PK_{\mathrm{RC}}, h, H, \hat{e}\}$.

4.2. Registration. This phase consists of the doctor registration and the patient registration. The process of registration is explained as follows:

Doctor registration: when a doctor D_i wants to login to the system to get the patient's information, he/she must first register at RC through the following steps:

Step DR-1: the doctor D_i chooses his/her own identification DID_i and password DPW_i and a random number r_i and then computes $h(r_i \oplus DPW_i)$. Then, D_i sends the message $\{DID_i, h(r_i \oplus DPW_i)\}$ to RC via a secure channel.

Step DR-2: upon receiving the message $\{DID_i, h(r_i \oplus DPW_i)\}$, RC computes $A_i = h(DI\ D_i|v)$, $B_i = h(A_i)$, $V_i = A_i \oplus h(DID_i \,||\, h(r_i \oplus DPW_i))$. Then, RC regards the parameter $s_{Di} = h(r_i \oplus DPW_i)$ as the doctor D_i's master key and then computes the corresponding public key $PK_{Di} = s_{Di} \cdot u \cdot P$.

Step DR-3: RC provides a license to the doctor D_i: $L_{Di} = s_{Di} \cdot v \cdot P$, then RC maintains $<DID_i, L_{Di}>$ in the checklist. This checklist is used to check the actual identity of the doctor when the doctor makes any dispute or misbehavior.

Step DR-4: the RC issues a smart card to the doctor D_i, the card contains the values $\{B_i, V_i, PK_{Di}, L_{Di}, r_i\}$. After receiving the smart card, the doctor D_i inserts the value r_i into the smart card. Then, the smart card contains $\{B_i, V_i, PK_{Di}, L_{Di}, r_i\}$.

Patient registration: when the patient P_j is ready to go to the hospital for treatment, RC will register his/her handheld terminal and assign relevant medical sensors to him/her to monitor the physical parameters.

Step PR-1: RC chooses a random number $s_{Pj} \in Z^*p$ as the patient P_j's master key. And then RC computes the corresponding public key $PK_{Pj} = s_{Pj} \cdot u \cdot P$. Next, RC sends the message $\{s_{Pj}, PK_{Pj}\}$ to the patient P_j through a secure channel.

4.3. Anonymous Authentication

4.3.1. Patient to Doctor Anonymous Authentication. When the patient P_j wants to send the data collected by himself to the doctor D_i to facilitate the doctor's diagnosis or detection, this step is required. Since the data transmitted by the patient to the doctor contain very sensitive health information, in order to preserve the privacy of these data, the patient needs to use encryption and authentication methods to process the data. The detailed steps are as follows:

Step PA-1: the patient P_j first chooses a random value $k \in Z^*p$ and calculates

$$\begin{aligned} a_1 &= k \cdot P, \\ a_2 &= k \cdot PK_{Di}, \\ a_3 &= h(\text{data})k \cdot s_{Pj} \cdot PK_{\mathrm{RC}}, \\ a_4 &= k \cdot PK_{Pj}, \\ w_1 &= (\text{data}a3a4Tj), \\ c_1 &= w1 \oplus H(a_2), \end{aligned} \tag{3}$$

where data are the physical parameters of the patient P_j and T_j is the timestamp. Then, the patient P_j sends the message $\{a_1, c_1, T_j\}$ to the doctor D_i via common channel.

Step PA-2: upon receiving the message $\{a_1, c_1, T_j\}$, the doctor D_i computes $w^*1 = c_1 \oplus H(s_{Di} \cdot a_1)$ and extracts

Table 1: Notation and its description.

Notation	Description
D_i	The ith doctor
DID_i	The identity of the ith doctor
PK_{Di}	The ith doctor's public key
RC	The registration center
PK_{RC}	The public key of RC
P_j	The jth patient
PID_j	The identity of the jth patient
$h(\cdot)$	A secure hash function, where h: $\{0,1\}^* \Rightarrow Z_q^*$
$H(\cdot)$	A hash function, where H: $E_p(a,b) \Rightarrow \{0,1\}^l$, in which l is the length of the string
$\hat{e}(\cdot,\cdot)$	A bilinear map $\hat{e}$: $G_1 \times G_1 \longrightarrow G_2$
$\|\|$	String concatenation operation
$\oplus$	The bitwise XOR operation

the *data*, a_3, a_4 and the timestamp T_j from w^*1. Then, the doctor D_i verifies whether the timestamp T_j is fresh. If it is not fresh, the doctor D_i discards the message directly and terminates the authentication process. Otherwise, go to the next step.

Step PA-3: the doctor D_i checks if $\hat{e}(a_3, PK_{Di})? = \hat{e}(PK_{\mathrm{RC}}, h(\mathrm{data}) \cdot s_{Di} \cdot a_4)$ holds. If the above equation is true, the doctor D_i considers that the patient P_j is legitimate and the health information *data* have not been destroyed. Otherwise, the patient P_j is considered to be an illegal user and refuses to accept the health information data.

Figure 2 summarizes the process of patient to doctor authentication phase.

Proof of Correctness. The challenger equation $\hat{e}(a_3, PK_{Di})? = \hat{e}(PK_{\mathrm{RC}}, h(\mathrm{data}) \cdot s_{Di} \cdot a_4)$ calculated by the doctor D_i should be held by using the values a_3 and a_4 sent from the patient P_j.

$$\begin{aligned}\hat{e}(a_3, PK_{Di}) &= \hat{e}\left(h(\mathrm{data}) \cdot k \cdot s_{Pj} \cdot PK_{\mathrm{RC}}, PK_{Di}\right)\\ &= \hat{e}\left(k \cdot s_{Pj} \cdot PK_{\mathrm{RC}}, h(\mathrm{data}) \cdot s_{Di} \cdot P\right)\\ &= \hat{e}\left(PK_{\mathrm{RC}}, h(\mathrm{data}) \cdot k \cdot s_{Pj} \cdot s_{Di} \cdot P\right)\\ &= \hat{e}\left(PK_{\mathrm{RC}}, h(\mathrm{data}) \cdot s_{Di} \cdot k \cdot PK_{Pj}\right)\\ &= \hat{e}\left(PK_{\mathrm{RC}}, h(\mathrm{data}) s_{Di} \cdot a_4\right).\end{aligned} \tag{4}$$

4.3.2. Doctor to Patient Anonymous Authentication. When the doctor D_i wants to get the relevant health data of the patient P_j, he first generates the query information *demand* and completes the message authentication through the following steps:

Step DA-1: the doctor D_i first inserts his/her smart card to a terminal and then inputs his/her identity DID_i and password DPW_i. Then, the smart card computes as follows:$A_i^* = h(DI\ D_i h(r_i \oplus DP\ W_i)) \oplus V_i$, $B_i^* = h(A_i^*)$, and checks whether $B_i^* = B_i$. If not, the smart card rejects this request and prompts the doctor to enter the correct identity and password. Otherwise, go to the next step.

Step DA-2: the doctor D_i chooses a random number $r \in Z^* p$ and computes

$$\begin{aligned}b_1 &= r \cdot P,\\ b_2 &= r \cdot PK_{Pj},\\ b_3 &= h(\mathrm{demand})\, r \cdot s_{Di} \cdot PK_{\mathrm{RC}},\\ b_4 &= r \cdot PK_{Di},\\ b_5 &= h(T_i) \cdot s_{Di} \cdot P,\\ Cert_i &= (L_{Di} T_i) \oplus H(h(T_i) \cdot s_{Di} \cdot PK_{\mathrm{RC}}),\\ w_2 &= (\mathrm{demand} b_3 b_4 Cert_i T_i),\\ c_2 &= w_2 \oplus H(b_2),\end{aligned} \tag{5}$$

where demand is the query request information of the doctor and T_i is the timestamp. Then, the doctor D_i sends the message $\{b_1, b_5, c_2, Cert_i, T_i\}$ to the patient P_j via a common channel.

Step DA-3: upon receiving the message $\{b_1, b_5, c_2, Cert_i, T_i\}$, the patient P_j verifies whether the time stamp T_i is fresh. If not, the authentication process is terminated. Otherwise, P_j uses his/her private key to compute $b_2^* = s_{Pj} \cdot b_1$, $w_2^* = c_2 \oplus H(b_2^*)$. And then, P_j extracts variables demand, b_3, b_4, $Cert_i$ and the timestamp T_i from w^{*2}.

Step DA-4: P_j verifies whether the equation $\hat{e}(b_3, PK_{Pj})? = \hat{e}(PK_{\mathrm{RC}}, h(\mathrm{demand}) \cdot s_{Pj} \cdot b_4)$ holds. If the above equation is true, the patient P_j considers the doctor to be a legitimate doctor, and he will provide the relevant health data according to the doctor's requirements. Otherwise, he believes that the doctor D_i is an illegal doctor and refuses to accept his request.

Figure 3 summarizes the process of login and the doctor to patient authentication phase.

Proof of correctness:

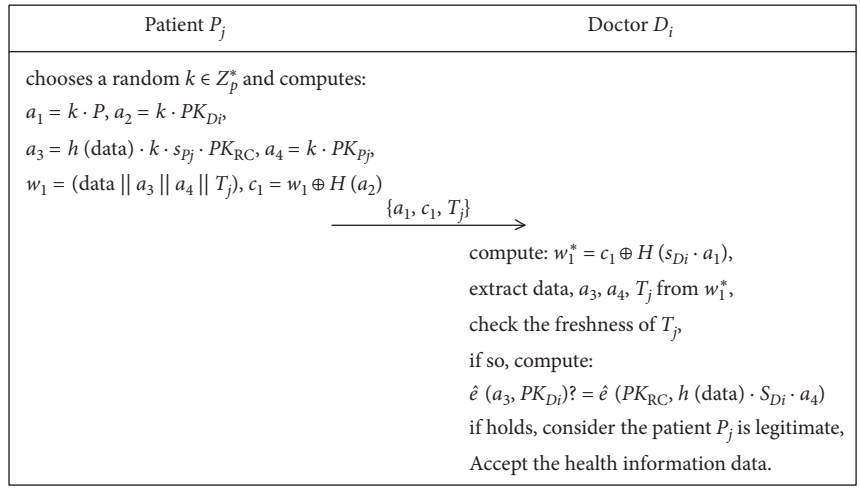

Figure 2: The patient to doctor authentication phase.

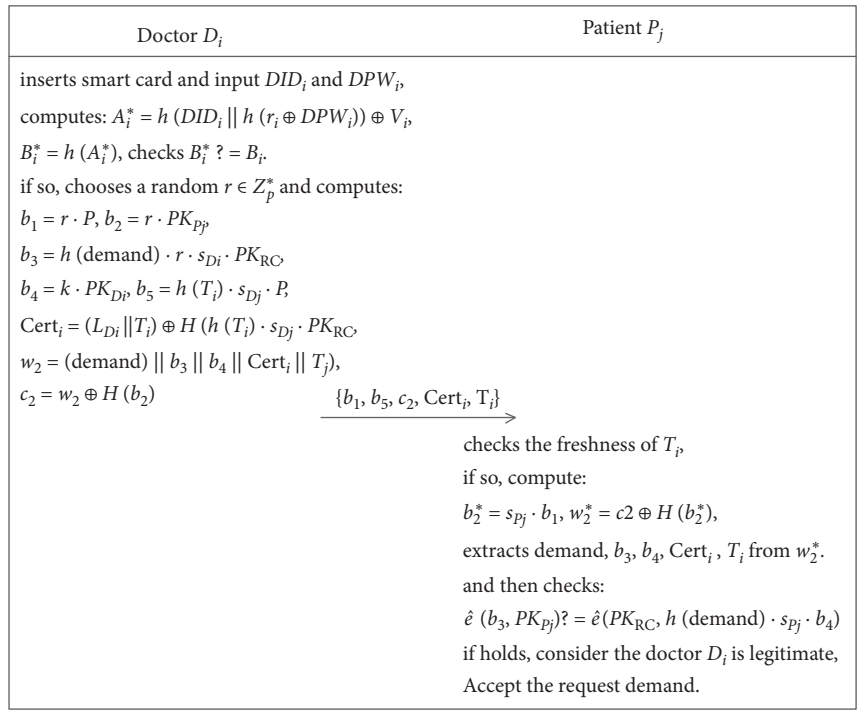

Figure 3: The login process and doctor to patient authentication phase.

$$\begin{aligned}\hat{e}\left(b_3, PK_{Pj}\right) &= \hat{e}\left(h(\text{demand}) \cdot r \cdot s_{Di} \cdot PK_{RC}, s_{Pj} \cdot P\right) \\ &= \hat{e}\left(PK_{\text{RC}}, h(\text{demand}) \cdot r \cdot s_{Di} \cdot s_{Pj} \cdot P\right) \\ &= \hat{e}\left(PK_{\text{RC}}, h(\text{demand}) \cdot s_{Pj} \cdot r \cdot s_{Di} \cdot P\right) \\ &= \hat{e}\left(PK_{\text{RC}}, h(\text{demand}) \cdot s_{Pj} \cdot b_4\right).\end{aligned} \tag{6}$$

Step DA-5 (*identity tracking*): if the request message *demand* is suspected of having a problem or illegal operation, RC is able to track the actual identity of the doctor using the certificate $Cert_i$ in the message. The process is as follows:

Then, RC finds the corresponding record $<DID_i, L_{Di}>$ in the checklist and gets the actual identity of the doctor DID_i.

$$\begin{aligned}&Cert_i \oplus H\left(s_{\text{RC}} \cdot b_5\right) \\ &= \left(L_{Di} T_i\right) \oplus H\left(h\left(T_i\right) \cdot s_{Di} \cdot PK_{\text{RC}}\right) \oplus H\left(s_{\text{RC}} \cdot b_5\right) \\ &= \left(L_{Di} T_i\right) \oplus H\left(h\left(T_i\right) \cdot s_{Di} \cdot PK_{\text{RC}}\right) \oplus H\left(s_{\text{RC}} \cdot h\left(T_i\right) \cdot s_{Di} \cdot P\right) \\ &= \left(L_{Di} T_i\right).\end{aligned} \tag{7}$$

5. Security Analysis

In this section, we first prove that the proposed anonymous user authentication protocol is provably secure under the BAN logic [32, 33]. Next, the security and functional features of the proposed authentication protocol are discussed.

5.1. BAN Logic-Based Formal Security Analysis. We use BAN logic to analyze the security and correctness of our proposed authentication protocol. Table 2 summarizes the notations and rules of the BAN logic.

Goals. According to the analytic procedures of the BAN logic, the proposed authentication protocol must satisfy the following security goals:

Goal_1: $P_j| \equiv D_i| \equiv P_j \overset{c_1}{\leftrightarrow} D_i$

Goal_2: $D_i| \equiv P_j| \equiv D_i \overset{c_2}{\leftrightarrow} P_j$

The initial status forms of the proposed authentication protocol are formally described as follows:

A_1: $D_i| \equiv \#(T_i, r)$

A_2: $P_j| \equiv \#(T_j, k)$

A_3: $D_i \triangleleft \{a_3, \text{data}\}_{H(a_2)}$

A_4: $P_j \triangleleft \{\text{demand}, T_i\}_{H(b_2)}$

The idealized transformed message of the proposed authentication protocol is described as follows:

Msg_1: $P_j \longrightarrow D_i$: $\{a_1, c_1, T_j\}$

Msg_2: $D_i \longrightarrow P_j$: $\{b_1, b_5, c_2, \text{Cert}_i, T_i\}$

The main analysis steps of the proposed authentication protocol based on the BAN logic are described as follows:

By A_2, A_3, and the message meaning rule, it is easy to getS_1: $D_i| \equiv P_j| \sim \{a_3, \text{data}\}_{H(a_2)}$

By S_1, A_3, Msg_1, and the nonce verification rule in which k is the necessary part of $H(a_2)$, it is easy to get S_2: $P_j| \equiv D_i| \equiv P_j \overset{H(a_2)}{\leftrightarrow} D_i$

By S_2, Msg_1, and the nonce verification rule in which T_j is the part of c_1, it is easy to get S_3: $P_j| \equiv D_i| \equiv P_j \overset{c_1}{\leftrightarrow} D_i$ (Goal_1)

By A_1, A_4, and the message meaning rule, it is easy to get S_4: $P_j| \equiv D_i| \sim \{b_5, c_2, T_i\}_{H(b_2)}$

By S_4, A_4, Msg_1, and the nonce verification rule in which r is the necessary part of $H(b_2)$, it is easy to get S_5: $D_i| \equiv P_j| \equiv D_i \overset{H(b_2)}{\leftrightarrow} P_j$

By S_5, Msg_2 and the nonce verification rule in which T_i is the part of c_2, it is easy to get S_6: $D_i| \equiv P_j| \equiv D_i \overset{c_2}{\leftrightarrow} P_j$ (Goal_2)

5.2. Informal Security Analysis. In this section, the security and functional features of the proposed authentication protocol are discussed. Through the detailed analysis, it has been proven that the proposed protocol can withstand various common attacks.

5.2.1. Privileged Insider Attack. In the proposed protocol, RC does not store any patient-related information. Therefore, the privileged insider cannot obtain any critical information about the patient. In another, although RC stores the doctor's checklist $<DID_i, L_{Di}>$ to track the doctor's true identity, the privileged insider cannot guess the doctor's password DPW_i or private key s_{Di}. Therefore, he/she has no advantage in breaking the robustness of the proposed authentication protocol.

5.2.2. Replay Attack. Owing to the open nature of the wireless communication channel, the replay attack poses a great security threat to the wireless body area networks. According to the specification of the proposed protocol, the first step of each entity (the patient or doctor) is to check the freshness of the authentication messages using the timestamps T_i or T_j. In addition, the timestamp is hashed and Exclusive OR ($\oplus$) with other parameters (c_1, c_2, or b_5), which is contained in the authentication messages. Therefore, if the timestamp is not fresh, the receiver discards the message directly and aborts the session. If the adversary modifies the timestamp, he/she cannot calculate the corresponding parameters. Consequently, our proposed protocol is able to withstand the reply attack.

5.2.3. Impersonation Attack. Let A be an adversary and he has the ability to intercept the authentication message of the patient P_j: $\{a_1, c_1, T_j\}$. A may try to generate a forged authentication message $\{a^*1, c^*1, T^*1\}$. Since A has not registered at RC and does not know the secret value u, it is impossible for A to obtain its own correct public key PK^*Pj. Even though the adversary A chooses a new random number k^* to the corresponding parameter a^*1, he cannot compute the correct parameters a^*3 and a^*4. Therefore, it is easy to find that the adversary cannot pretend to be a patient.

Similarly, we can get that the adversary A has no ability to pretend to be a doctor because he does not know the RC's secret value u. Therefore, the proposed authentication protocol can resist the impersonation attack.

5.2.4. Stolen Smart Card Attack. In the proposed protocol, every doctor has a smart card to login to the wireless body area networks. Suppose an adversary A picks up or steals a doctor's smart card and extracts the stored secret parameters $\{B_i, V_i, PK_{Di}, L_{Di}, r_i\}$, where $B_i = h(A_i)$, $V_i = A_i \oplus h(DID_i \,||\, h(r_i \oplus DPW_i))$, $PK_{Di} = s_{Di} \cdot u \cdot P$, and $L_{Di} = s_{Di} \cdot v \cdot P$. Furthermore, assume that the adversary A eavesdrops the authentication message $\{b_1, b_5, c_2, Cert_i, T_i\}$ sent by the doctor. Using these obtained parameters, if A wants to pretend to be a doctor and launch an attack, he must try to guess the doctor's password DPW_i to generate the doctor's private key $s_{Di} = h(r_i \oplus DPW_i)$. Without knowing the doctor's password, the adversary A cannot compute the doctor's private key. Then he cannot further generate the correct authentication message. Therefore, it is easy to find that the proposed protocol is resistant to stolen smart card attack.

Table 2: The notations and rules of the BAN logic.

Notations	Description
P, Q	A principal
$P \lhd X$	P sees X
$P\vert\sim X$	P said X, X was send by P
$P\vert\Rightarrow X$	P has jurisdiction over X
$\longrightarrow^{k} P$	k is P's public key
$P \overset{k}{\leftrightarrow} Q$	k is only known to P and Q.
$\#(X)$	X is fresh
$<X>_k$	Formulae X is combined with the formulae k
$\{X\}_k$	X is encrypted by the key k
$P\vert\equiv X$	P has faith in the truth of X
Rule 1: message meaning rule	$(P\vert\equiv P \overset{k}{\leftrightarrow} Q, P\lhd\langle X\rangle_k)/(P\vert\equiv Q\vert\sim X)$ or $(P\vert\equiv \longrightarrow^{k} Q, P\lhd\{X\}_k)/(P\vert\equiv Q\vert\sim X)$
Rule 2: nonce verification rule	$(P\vert\equiv \#(X), P\vert\equiv Q\vert\sim X)/(P\vert\equiv Q\vert\equiv X)$
Rule 3: jurisdiction rule	$(P\vert\equiv Q\Rightarrow X, P\vert\equiv Q\vert\equiv X)/(P\vert\equiv X)$
Rule 4: decomposition rule	$P\vert\equiv Q\vert\equiv (X, Y)/(P\vert\equiv Q\vert\equiv X)$

5.2.5. User Anonymity. User anonymity is a very important security requirement in the WBAN. To protect the privacy of doctors and patients, the proposed protocol has made the following measures. In the patient side, the random value $k \in Z^* p$ and the timestamp T_j are used in each round of the patient to doctor authentication. The patient's master key s_{Pj} and public key PK_{Pj} are encrypted in a_3, a_4 with k and T_j, respectively. Suppose that the adversary A could intercept the message $\{a_1, c_1, T_j\}$, it is an impossible task for to obtain the patient's fixed master key s_{Pj} and public key PK_{Pj}. Similarly, the adversary A cannot use the message transferred from the doctor to the patient to obtain the doctor's fixed parameters. Consequently, the proposed authentication protocol can achieve the anonymity of the patients and the doctors.

5.2.6. Authentication and Data Integrity. In the proposed scheme, the patient's physiological parameter data and the doctor's query request information demand are encrypted by the hash values $H(a_2)$ and $H(b_2)$, respectively. In addition, the values h(data) and h(demand) are the parameters of a_3 and b_3, respectively. According to the property of hash, if any bits are modified, the verify equations $\widehat{e}(a_3, PK_{Di})? = \widehat{e}(PK_{\mathrm{RC}}, h(\mathrm{data}) \cdot s_{Di} \cdot a_4)$ and $\widehat{e}(b_3, PK_{Pj})? = \widehat{e}(PK_{\mathrm{RC}}, h(\mathrm{demand}) \cdot s_{Pj} \cdot b_4)$ cannot be established. Consequently, the proposed authentication protocol can check the integrity of the messages transmitted between the doctor and the patient.

5.2.7. Unlinkability and Conditional Traceability. For the adversary A, he could intercept the messages $\{a_1, c_1, T_j\}$ and $\{b_1, b_5, c_2, Cert_i, T_i\}$. However, the random numbers k and r are different in each round of the message authentication. Therefore, it is difficult for the adversary A to trace the messages which were transmitted from the doctor or the patient. On the other hand, the RC has the ability to track the doctor's actual identity through the formula in Step DA-5. Therefore, except for the ability of RC to track the identity of doctors, other entities cannot track the identity of doctors or patients.

6. Performance Analysis

In this section, the performance of the proposed scheme is evaluated in terms of computational cost, and communication overhead, and security requirements. We then compare the proposed scheme with the existing research activities in terms of security and functional features.

6.1. Computation Cost. In the proposed scheme, the computational cost isreferred to the time which was consumed in the phase of message generation and verification. The multiplicative cyclic groups used in the proposed scheme are built based on a Type-A elliptic curve, which is defined in the pairing-based cryptography (PBC) library [34]. In addition, we use C language under specific IDE and C/CCC MIRACL Library to implement the related cryptographic operations. To evaluate the computational costs of the proposed scheme, some of the related notations are listed in Table 3.

Our implementation uses a PC with Intel Core i7 CPU 2.6 GHz and 8 GB memory to run the proposed authentication protocol. In our simulation, each randomized ID is 1024 bits, and the size of the ECC point is 160 bits. The execution time for each cryptographic operation is derived after 10 times experiments. The average running time of each cryptographic operation is listed in Table 4. It needs to be explained here that we have ignored the running time of the XOR operation because it is negligible.

In our implementation, the costs of the registration and smart card distribution are not considered since it only runs a limited number of times in the initial stage of the proposed protocol. Table 5 shows a comparison for computation cost between the proposed authentication protocol and the related works. From Table 5, it is obvious that the proposed authentication protocol takes only one point multiplication, one pairing, and one hash function to generate the certificate. And the time of verifying the certificate only needs one hash function, two point multiplication, and one pairing operation. Compared with the related research activities, it is easy to find that the proposed protocol needs a very low computational overhead to complete the authentication process.

Table 3: Execution time of the related pairing-based operations.

Notations	Execution time for various operations
T_h	One-way hash function $H(\cdot)$ or $h(\cdot)$
T_{pair}	Bilinear pairing computation
T_{add}	Addition operation of points in ECC
T_{exp}	Exponential operation
T_{mul}	Scalar multiplication of elliptic curve
T_{en}	Symmetric encryption algorithm AES (128-bit key)

Table 4: Execution time of the related pairing-based operations.

Encryption element	T_h (ms)	T_{pair} (ms)	T_{add} (ms)	T_{exp} (ms)	T_{mul} (ms)	T_{en} (ms)
Running time	<1	3.61	<1	2.74	1.63	<1

Table 5: Execution time of the related pairing-based operations.

Schemes	Time of generating the certificate	Time of verifying the certificate
Wu et al.'s scheme	$3T_h + 4T_{\text{mul}} + T_{\text{en}}$	$4T_h + 4T_{\text{mul}} + T_{\text{pair}} + T_{\text{en}}$
Shen et al.'s scheme	$T_h + 3T_{\text{mul}}$	$T_h + 4T_{\text{pair}} + T_{\text{en}} + 2T_{\text{mul}}$
Das et al.'s scheme	$5T_h + 2T_{\text{en}}$	$4T_h + 2T_{\text{en}}$
Liu et al.'s scheme	$2T_{\text{pair}} + 3T_h + T_{\text{mul}}$	$3T_{\text{pair}} + 3T_h + 3T_{\text{mul}}$
Proposed scheme	$T_h + T_{\text{mul}} + T_{\text{pair}}$	$T_h + 2T_{\text{mul}} + T_{\text{pair}}$

6.2. Communication Overhead. To analyze the communication overhead of the proposed authentication protocol, the size of the parameters used in the proposed scheme is shown below. The length of the random number, the point of ECC, the identity, the output of a hash function, and the timestamp are 128 bits, 320 bits, 128 bits, 160 bits, and 32 bits, respectively. We assumed that the length of the physical parameters of the patient *data* and the query request information of the doctor *demand* are 500 bits and 300 bits, respectively.

Under these deliberations, in the patient to doctor authentication phase of the proposed protocol, the patient sends the message $M_1 = \{a_1, c_1, T_j\}$ to the doctor. Similarly, in the doctor to patient authentication phase, the doctor sends the message $M_2 = \{b_1, b_5, c_2, Cert_i, T_i\}$ to the doctor. These two messages need $320 + 500 + 320 + 320 + 32 + 32 = 1524$ bits and $320 + 320 + 300 + 320 + 32 = 1292$ bits, respectively. In Table 6, we summarize the brief comparison of communication overhead between the proposed scheme and other existing schemes.

Compared with other existing schemes, the proposed scheme's communication cost is similar to that of other related research works. However, the messages in the proposed protocol contain the patient's physical parameter data and the doctor's query request information demand. In other words, the proposed scheme can not only achieve the identity authentication, but also complete the transfer of the patient's physiological data and the data requested by the doctor. Therefore, the proposed protocol is not only efficient in terms of communication overhead in the WBAN system but also has more extra features.

Table 6: The comparison of communication cost in different schemes.

Scheme	Number of messages	Communication cost (bits)
Wu et al.'s scheme	3	2112
Shen et al.'s scheme	4	3040
Das et al.'s scheme	2	1536
Liu et al.'s scheme	4	3840
Proposed scheme	2	2816

Table 7: The comparison of security requirements.

Scheme	I_1	I_2	I_3	I_4	I_5	I_6	I_7
Wu et al.'s scheme	√	√	√	√	√	×	√
Shen et al.'s scheme	√	×	√	√	×	√	√
Das et al.'s scheme	√	√	√	×	√	√	×
Liu et al.'s scheme	√	√	√	√	×	√	√
Proposed scheme	√	√	√	√	√	√	√

Note. I_1: replay attack; I_2: impersonation attack; I_3: privileged insider attack; I_4: secure mutual authentication; I_5: message integrity and confidentiality; I_6: user privacy; I_7: loss of device attack.

6.3. Security Requirements. We compare the proposed authentication protocol with the related authentication schemes in terms of security requirements such as replay attack, impersonation attack, secure mutual authentication, message integrity, and confidentiality. The detailed comparison of various security attacks and functions is shown in Table 7. The comments from Table 7 show that our

authentication protocol not only gives the support of much more functionality but also overcomes more security weaknesses.

7. Conclusion

In this article, an efficient and privacy-preserving authentication protocol for the WBAN is presented. In the proposed authentication scheme, the doctor and the patient are anonymously authenticated by each other before sending the patient-related information (the patient's physical parameters or the doctor's query request). The security analysis showed that the proposed authentication protocol could provide resistance against common attacks such as replay attack, impersonation attack, and eavesdropping attack. The proposed authentication scheme takes very little cost for signature and certificate authentication, which is essential for the WBAN-based applications. Moreover, the proposed scheme gives an effective privacy and tracking method to disclose the actual identification of the malicious doctor to improve the usability of the WBAN. The performance analysis showed that the proposed scheme is efficient in terms of computational cost and communication cost. It is more appropriate for practical WBAN-based applications. The future extension of this article is to provide an authentication method that can transmit a larger amount of data for the patient in an efficient manner.

Data Availability

The data used to support the findings of this study are available at https://crypto.stanford.edu/pbc/.

Conflicts of Interest

None of the authors have any conflicts of interest.

Acknowledgments

This research was supported by the National Natural Science Foundation of China (Grant nos. 61772477 and U1804263) and the Key Scientific Research Projects of Colleges and Universities in Henan Province (no. 16A520075).

References

[1] S. H. Islam, M. Azees, N. Kumar et al., "Efficient and secure anonymous authentication with location privacy for IoT-based WBANs," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 4, pp. 2603–2611, 2020.

[2] M. Hussain, A. Mehmood, S. Khan et al., "Authentication techniques and methodologies used in wireless body area networks," *Journal of Systems Architecture*, vol. 101, 2019.

[3] M. Umar, Z. Wu, and X. Liao, "Mutual authentication in body area networks using signal propagation characteristics," *IEEE Access*, vol. 8, pp. 66411–66422, 2020.

[4] M. Shuai, L. Xiong, C. Wang, and N. Yu, "Lightweight and privacy-preserving authentication scheme with the resilience of desynchronisation attacks for WBANs," *IET Information Security*, vol. 14, no. 4, pp. 380–390, 2020.

[5] X. Liu, R. Zhang, and M. Zhao, "A robust authentication scheme with dynamic password for wireless body area networks," *Computer Networks*, vol. 161, pp. 220–234, 2019.

[6] V. Odelu, S. Saha, R. Prasath, L. Sadineni, M. Conti, and M. Jo, "Efficient privacy preserving device authentication in WBANs for industrial e-health applications," *Computers & Security*, vol. 83, pp. 300–312, 2019.

[7] K.-A. Shim, "Universal forgery attacks on remote authentication schemes for wireless body area networks based on Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9211-9212, 2019.

[8] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," *IEEE Systems Journal*, vol. 9, no. 3, pp. 816–823, 2015.

[9] S. Chatterjee, A. K. Das, and J. K. Sing, "A novel and efficient user access control scheme for wireless body area sensor networks," *Journal of King Saud University–Computer and Information Sciences*, vol. 26, no. 2, pp. 181–201, 2014.

[10] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for WirelessBody area networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 332–342, 2014.

[11] T.-F. Lee and M. Chen, "Lightweight identity-based group key agreements using extended chaotic maps for wireless sensor networks," *IEEE Sensors Journal*, vol. 19, no. 22, pp. 10910–10916, 2019.

[12] A. K. Das, S. Chatterjee, and J. K. Sing, "A new biometric-based remote user authentication scheme in hierarchical wireless body area sensor networks," *Ad Hoc and Sensor Wireless Networks*, vol. 28, no. 3-4, pp. 221–256, 2015.

[13] C. Wang and Y. Zhang, "New authentication scheme for wireless body area networks using the bilinear pairing," *Journal of Medical Systems*, vol. 39, no. 11, p. 136, 2015.

[14] H. Debiao, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2590–2601, 2017.

[15] J. Liu, L. Zhang, and R. Sun, "1-RAAP: an efficient 1-round anonymous authentication protocol for wireless body area networks," *Sensors*, vol. 16, no. 5, p. 728, 2016.

[16] X. Li, J. Peng, F. Wu, M. Karuppiah, and K.-K. Raymond Choo, "An enhanced 1-round authentication protocol for wireless body area networks with user anonymity," *Computers & Electrical Engineering*, vol. 61, pp. 238–249, 2017.

[17] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," *Future Generation Computer Systems*, vol. 78, no. 3, pp. 956–963, 2018.

[18] X. Liu, C. Jin, and F. Li, "An improved two-layer authentication scheme for wireless body area networks," *Journal of Medical Systems*, vol. 42, no. 8, pp. 143–154, 2018.

[19] M. Wazid, A. K. Das, and A. V. Vasilakos, "Authenticated key management protocol for cloud-assisted body area sensor networks," *Journal of Network and Computer Applications*, vol. 123, pp. 112–126, 2018.

[20] S. Qiu, G. Xu, H. Ahmad, and L. Wang, "A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems," *IEEE Access*, vol. 6, pp. 7452–7463, 2017.

[21] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," *Journal of Network and Computer Applications*, vol. 106, no. 6, pp. 117–123, 2018.

[22] M. Shuai, B. Liu, N. Yu, L. Xiong, and C. Wang, "Efficient and privacy-preserving authentication scheme for wireless body area networks," *Journal of Information Security and Applications*, vol. 52, Article ID 102499, 2020.

[23] M. Fotouhi, M. Bayat, A. Das, H. Far, S. Pournaghi, and M. A. Doostari, "A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT," *Computer Networks*, vol. 177, Article ID 107333, 2020.

[24] D. Kumar, H. S. Grover, and Adarsh, "A secure authentication protocol for wearable devices environment using ECC," *Journal of Information Security and Applications*, vol. 47, pp. 8–15, 2019.

[25] S. Jegadeesan, M. Azees, N. Ramesh Babu, U. Subramaniam, and J. D. Almakhles, "EPAW: efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (WBANs)," *IEEE Access*, vol. 8, pp. 48576–48586, 2020.

[26] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[27] B. Narwal and A. K. Mohapatra, "A survey on security and authentication in wireless body area networks," *Journal of Systems Architecture*, vol. 113, Article ID 101883, 2020.

[28] J. Cui, X. Zhang, H. Zhong, J. Zhang, and L. Liu, "Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1654–1667, 2020.

[29] W. Tan, J. Zhang, Y. Zhang et al., "A PUF-based and cloud-assisted lightweight Authentication for multi-hop body area network," *Tsinghua Science and Technology*, vol. 26, no. 1, pp. 36–47, 2021.

[30] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K.-K. R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Computer Networks*, vol. 129, pp. 429–443, 2017.

[31] J. Zhang, L. He, Q. Zhang et al., "Pseudonym-based privacy protection scheme for participatory sensing with incentives," *Ksii Transactions on Internet & Information Systems, vl.*vol. 10, no. 11, pp. 5654–5673, 2016.

[32] S. F. Aghili, H. Mala, P. Kaliyar, and M. Conti, "SecLAP: secure and lightweight RFID authentication protocol for medical IoT," *Future Generation Computer Systems*, vol. 101, pp. 621–634, 2019.

[33] Z. Ali, A. Ghani, I. Khan, S. A. Chaudhry, S. K. H. Islam, and D. Giri, "A robust authentication and access control protocol for securing wireless healthcare sensor networks," *Journal of Information Security and Applications*, vol. 52, pp. 1–14, Article ID 102502, 2020.

[34] B. Lynn, "Pbc library–the pairing-based cryptography library," 2007, https://crypto.stanford.edu/pbc/.