Hindawi
Security and Communication Networks
Volume 2019, Article ID 8145087, 14 pages
https://doi.org/10.1155/2019/8145087

Research Article

Lightweight and Secure Three-Factor Authentication Scheme for Remote Patient Monitoring Using On-Body Wireless Networks

Mengxia Shuai,[1] **Bin Liu**,[1] **Nenghai Yu**,[1] **and Ling Xiong**[2]

[1]*School of Information Science and Technology, University of Science and Technology of China, Hefei 230026, China*
[2]*School of Computer and Software Engineering, Xihua University, Chengdu 610039, China*

Correspondence should be addressed to Mengxia Shuai; smx12345@mail.ustc.edu.cn

Received 1 February 2019; Revised 28 April 2019; Accepted 15 May 2019; Published 2 June 2019

Guest Editor: Milena Radenkovic

On-body wireless networks (oBWNs) play a crucial role in improving the ubiquitous healthcare services. Using oBWNs, the vital physiological information of the patient can be gathered from the wearable sensor nodes and accessed by the authorized user like the health professional or the doctor. Since the open nature of wireless communication and the sensitivity of physiological information, secure communication has always been the vital issue in oBWNs-based systems. In recent years, several authentication schemes have been proposed for remote patient monitoring. However, most of these schemes are so susceptible to security threats and not suitable for practical use. Specifically, all these schemes using lightweight cryptographic primitives fail to provide forward secrecy and suffer from the desynchronization attack. To overcome the historical security problems, in this paper, we present a lightweight and secure three-factor authentication scheme for remote patient monitoring using oBWNs. The proposed scheme adopts one-time hash chain technique to ensure forward secrecy, and the pseudonym identity method is employed to provide user anonymity and resist against desynchronization attack. The formal and informal security analyses demonstrate that the proposed scheme not only overcomes the security weaknesses in previous schemes but also provides more excellent security and functional features. The comparisons with six state-of-the-art schemes indicate that the proposed scheme is practical with acceptable computational and communication efficiency.

1. Introduction

With the improvement of living standards and the rapid development of public health, the life expectancy of humans has increased rapidly over the past decades. For example, the average life expectancy of Australian is 70.8 years old in 1960, but it has risen to 81.7 years old in 2010 [1]. With increasing age, lots of elderly people may suffer from various types of chronic diseases and unable to take care of themselves, and these will lead to a heavy burden to the next generations and the healthcare system. To handle this challenge, remote monitoring has emerged as an effective solution for the healthcare system [2, 3]. On-body wireless networks (oBWNs), as an important part of remote monitoring system, have received a great deal of attention from researchers in the academic and industrial field because of its potential to improve the quality of healthcare services.

A typical architecture for remote patient monitoring using oBWNs is demonstrated in Figure 1, which is adapted from the schemes [4–6]. In this scenario, there are four kinds of participants: registration authority (*RA*), the user, gateway node (*GWN*), and wearable sensor nodes. The *RA* is a trusted third party, who is in charge of generating system parameters and the registration of all the users, *GWN*, and wearable sensor nodes. The user, such as health professional or the doctor, can access the life-critical data of target patient and provide real-time support and interventions. *GWN*, which has high computation and communication capabilities, is the critical intermediary between the user and the wearable sensor nodes. The wearable sensor nodes, such as blood pressure sensor, cardiosensor, and pulse sensor, deploy around/on the patient's body and collect vital physiological information of target patient. Using oBWNs, it is possible to provide the

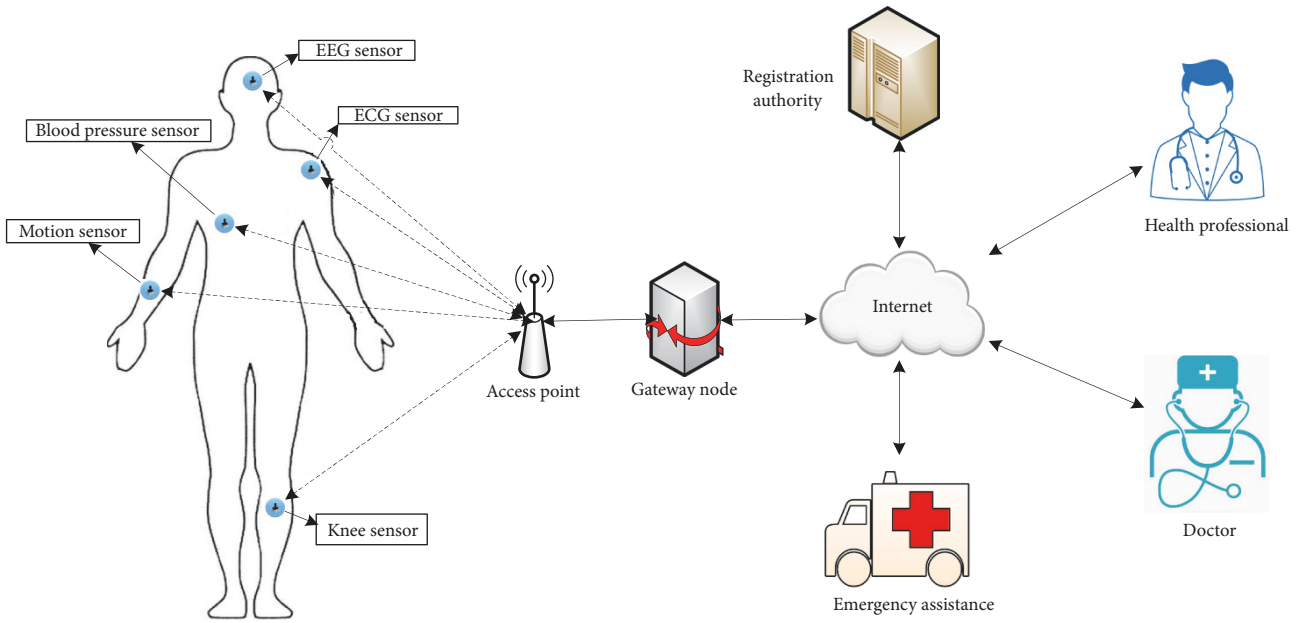

Figure 1: The communication architecture for remote patient monitoring using oBWNs.

continue and real-time monitoring of the patient, regardless of the patient's location.

Although oBWNs greatly improve the health outcomes and quality of life, the open wireless network environment makes the application of oBWNs face many security risks and threats. A malicious adversary can intercept, modify, insert, and delete the transmitted messages over insecure public communication channel easily [7]. In addition, it is extremely dangerous if the unauthorized users send instructions to stop the function of the wearable devices, especially the wearable devices that are critical to the life of the patient, like heart bumps. What is more, the sensitivity of the physiological data collected by wearable sensor nodes let privacy become a significant concern in oBWNs. Therefore, there is a great need to satisfy the requirements of confidentiality, integrity, and availability. Authentication is one of the efficient mechanisms to deal with trustworthy and authentic users. In the past several years, a large number of authentication schemes have been proposed to provide secure and effective healthcare monitoring of the patients using oBWNs. Since the wearable sensor nodes have weak energy and computation ability, authentication schemes based on public key encryption, such as elliptic curve cryptography (ECC) [8] and Rabin cryptosystem [9], have heavy computation burdens, and they are not suitable for realistic scenarios. Therefore, the method of using the lightweight operations, liking symmetric encryption/decryption and hash functions, is an effective way to deal with the weaknesses of public key encryption. However, after careful analysis, we find that most of these existed schemes using lightweight cryptographic primitives are so susceptible to security threats and not suitable for practical use. Specifically, all these schemes fail to provide forward secrecy and suffer from the desynchronization attack.

1.1. Related Work. Authentication is an essential security measure for the authorized user to access the patient's sensitive information collected by wearable sensor nodes. Until now, lots of lightweight and effective authentication schemes had been proposed for healthcare applications. In 2012, an efficient and lightweight authentication scheme, named E-SAP, was proposed by Kumar et al. [10] for healthcare applications using wireless medical sensor networks (WMSNs). They claimed that the scheme was secure and resisted multiple types of attacks. Unfortunately, He et al. in 2013 [11] indicated that the scheme in [10] failed to provide user anonymity. Moreover, their scheme was vulnerable to the privileged-insider attack and the off-line password guessing attack. To conquer the mentioned weaknesses, they presented a robust and efficient authentication scheme for healthcare applications using WMSNs. However, a series of articles [12–14] pointed out that the scheme in He et al. [11] still had some drawbacks and flaws, such as user impersonation attack, sensor node capture attack, off-line password guessing attack, forward secrecy attack, and lack of wrong password detection mechanism. Later, Srinivas et al. in 2017 [15] pointed out that the scheme in [12] suffered from stolen smart card attack, insider attack and user impersonation attack. To handle these drawbacks, an authentication scheme using only computationally efficient operations was proposed for WMSNs. Later, Das et al. in 2017 [16] indicated that user anonymity was not provided in the scheme [14]. In addition, the scheme in [14] could not withstand sensor node capture attack and privileged-insider attack. To overcome the security weaknesses, they presented an efficient and secure authentication scheme for WMSNs and claimed that the enhanced scheme was secure against possible known attacks and offered additional functionality features. In 2017, Wu et al. [4] deemed that the scheme in [15] had weaknesses

such as off-line password guessing attacks, and they were impractical if running. To overcome the historical security problems, a novel and lightweight two-factor authentication scheme for WMSNs was proposed, which provided user untraceability and met the desired security requirements. To ensure secure and authorized communication, Amin et al. in 2018 [5] presented an architecture for patient monitoring, and an anonymity and robust mutual authentication scheme was proposed. They claimed that their scheme was more robust and cost-effective than the existing schemes. But unluckily, Ali et al. in 2018 [6] showed that the scheme in [5] was vulnerable to user impersonation attack, off-line password guessing attack, and known session key temporary information attack. In addition, they proposed an enhanced three-factor authentication scheme for healthcare monitoring. In 2019, Chandrakar [17] presented a lightweight and robust two-factor authentication protocol for healthcare monitoring. Their scheme was efficient because only the hash function and bit XOR operations were used. Similar to some previous schemes, their scheme could not provide user anonymity and forward secrecy.

Many authentication schemes based on asymmetric cryptographic techniques were also proposed for patient monitoring in the past few years. In 2015, He et al. [18] discussed the overall system architecture and associated security requirements of a typical ambient assisted living system, and an efficient authentication protocol based on ECC was proposed subsequently. In order to provide secure communication for WMSNs, Hayajneh et al. [19] in 2016 presented a lightweight authentication scheme based on public key technology, and the Rabin cryptosystem was implemented with different hardware settings using a Tmote sky mote to prove its efficiency. In 2017, Liu and Chung [20] proposed a user authentication scheme and data transmission mechanism for medical monitoring based on wireless sensor networks, in which the cryptosystem based on bilinear pairing was used. Unfortunately, Challa et al. [8] in 2017 showed that the scheme in [20] was suspected to some desirable attributes, such as inappropriate mutual authentication and lacking of user anonymity. Besides, their scheme was vulnerable to many known attacks like stolen smart card attack, off-line password guessing attack, privileged-insider attack, and user impersonation attack. To counter these limitations and improve efficiency, they presented a three-factor authentication and key agreement scheme with provably secure for healthcare, in which the lightweight ECC point multiplications was used. In the same year, Jiang et al. [9] put forward an efficient and end-to-end authentication scheme based on quadratic residues for wearable health monitoring. In 2018, Jangirala et al. [21] proposed a new cloud based user authentication scheme for wearable healthcare monitoring system, in which the Rabin cryptosystem was used. Although these public key schemes improved the security of authentication in the IoT environment, these schemes should be avoided because the asymmetric-based solutions were highly computational and had memory overheads.

From the above analysis, we can see that though researchers proposed many lightweight authentication schemes for patient monitoring in the past, however, none of them provides both lightweight functionality and high security. The authentication schemes only using lightweight cryptographic primitives, such as the schemes in [4–6, 14, 15, 17], failed to provide forward secrecy and suffered from the desynchronization attack. This motivates us to design a lightweight authentication scheme for patient monitoring, which provides more security and functionality attributes.

1.2. Motivation and Contributions. In order to provide user anonymity and untraceability, the method of using pseudonym identity has been adopted in the schemes [4–6]. In this way, a randomly generated pseudonym identity, which is updated after each successful session, is stored in both the user and the *GWN* side, respectively. Owing to the difference of the pseudonym identity at each session, the specific user cannot be tracked. Unfortunately, Wang and Wang in 2015 [22] indicated that the use of pseudonym identity may lead to the problem of desynchronization attack, which may make the authentication scheme unusable unless the user or the wearable sensor node reregisters. On the other hand, the hash chain technology can be used to ensure forward secrecy for lightweight cryptographic schemes [23]. However, this technique can also lead to the desynchronization attack because both parties need to update their shared one-time hash chain value after the completion of each session.

Motivated by these insights and our previous research work [24], we presented a lightweight and secure three-factor authentication scheme for remote patient monitoring using oBWNs. Our contributions lie in the following aspects:

(1) We briefly review the authentication schemes for healthcare monitoring, and the security drawbacks of the schemes are pointed out. Specifically, we find that all the schemes using lightweight cryptographic primitives fail to provide forward secrecy and suffer from the desynchronization attack.

(2) We present a lightweight and secure three-factor authentication scheme for remote patient monitoring using oBWNs. The proposed scheme adopts the pseudonym identity method to achieve user anonymity, and one-time hash chain technique is employed to ensure forward secrecy. In order to resist against desynchronization attack on the communication between the user and the *GWN*, two pseudonym identities MID_{i0} and MID_{i1} are stored in the back-end of *GWN*, respectively. Specifically, the value of the new pseudonym identity is stored in MID_{i0}, and MID_{i1} has two functions: the first one is to store the identity of the old pseudonym, and the second one is using as a tag to update the hash chain. If MID_{i1} is NULL, it means that the value of the hash chain has been updated in the previous session. Otherwise, the value of hash chain has not been changed. In order to resist against desynchronization attack on the communication between the *GWN* and the wearable sensor node, serial number technique is used in our scheme. Finally, a symmetric session key *SK* is established between the user and the wearable sensor node, which is used for future secure communications.

(3) We give the formal security analysis under the widely accepted Burrows-Abadi-Needham (BAN) logic [25], and it proves that the proposed scheme achieves mutual authentication and the session key SK is mutually established between the user and the wearable sensor node with the assistance of GWN. In addition, the informal security analysis shows that the proposed scheme can not only achieve some excellent function features, but also resist various malicious attacks, such as desynchronization attack, mobile device loss attack, replay attack, and wrong password login attack. Furthermore, we evaluate the performance of the proposed scheme with six state-of-the-art schemes, and the results demonstrate that the proposed scheme is practical with acceptable computational and communication efficiency.

1.3. Organization of the Paper. The reminder of this paper is organized as follows. Section 2 briefly introduces the preliminary knowledge of authentication schemes for remote patient monitoring. Our proposed authentication scheme for remote patient monitoring is described in Section 3, followed by its security analysis in Section 4. The performance of the proposed scheme is evaluated with the state-of-the-art schemes in Section 5. Finally, Section 6 concludes this paper.

2. Preliminaries

This section introduces some basic knowledge, containing notations and abbreviations used in this paper, security requirements of user authentication scheme for remote patient monitoring using oBWNs, threat model, and basic information about biometrics fuzzy extractor.

2.1. Notations and Abbreviations. For convenience, all the notations and abbreviations mentioned in the proposed scheme are defined in Table 1.

Table 1: Notations and abbreviations.

Notation	Descriptions
RA	Registration authority
U_i	User
MD	Mobile device of U_i
GWN_j	Gateway node
SN_k	Wearable sensor node
ID_i	Unique identity of U_i
PW_i	Password of U_i
BIO_i	Biometric information of U_i
MID_i	Temporary identity of U_i
GID_j	Unique identity of GWN_j
SID_k	Unique identity of SN_k
R_1, R_2, R_3	Random number
NC_{k0}	Serial number in GWN_j side
NC_k	Serial number in SN_k side
K	Master secret key of GWN_j
SK	Session key
T_1	Time stamp values
ΔT	The maximum of the transmission delay time
$h(\cdot)$	One-way hash function
$X\|\|Y$	Concatenate operation
$\oplus$	XOR operation

2.2. Security Requirements. Ali et al. in 2018 [6] pointed out that the authentication scheme for remote patient monitoring should satisfy many security requirements, including strong user authentication, mutual authentication, confidentiality, session key establishment, low communication and computation cost, data freshness, and secure against different kinds of popular attacks, such as impersonation attack, replay attack, and password guessing attack. Due to the sensitivity of physiological data, we believe that an authentication scheme for remote patient monitoring should also meet the following security properties.

Forward Secrecy. The authentication scheme provides forward secrecy, which means that if an adversary acquires the long-term keys of the user, GWN, and the wearable sensor node, he/she cannot access the session keys generated in previous sessions. Conversely, if authentication scheme fails to provide forward secrecy, it may cause the disclosure of the session keys used in previous communications and the disclosure of the patient's sensitive information. To ensure the secure transmission of sensitive information, authentication scheme for remote patient monitoring should achieve forward secrecy.

Resistance to Desynchronization Attack. To the best of our knowledge, desynchronization attack has attracted little attention in the previous authentication schemes, and the damaging threat is ignored. However, the practicality and seriousness of desynchronization attack have been intensively discussed in the cryptography community [26]. Therefore, the proposed scheme should need an effective synchronization method to maintain the consistency of several one-time values among the user, GWN, and the wearable sensor node.

Quick Detection of Wrong Password. In network applications, user usually needs to manage lots of identity and password pairs. Therefore, a wrong password detection mechanism is required for user authentication. With the help of this mechanism, the MD can reject session initiated by wrong password quickly, and this process will save a lot of computational and communication cost.

2.3. Threat Model. When considering cryptanalysis of the user authentication schemes, Dolev-Yao threat model [27] is widely used. Under this model, the communications between any two communicating parties are over an insecure channel, and the endpoint entities should not be considered as trusted entities. Based on this threat model, an adversary $\mathcal{A}$ is supposed to have the following abilities:

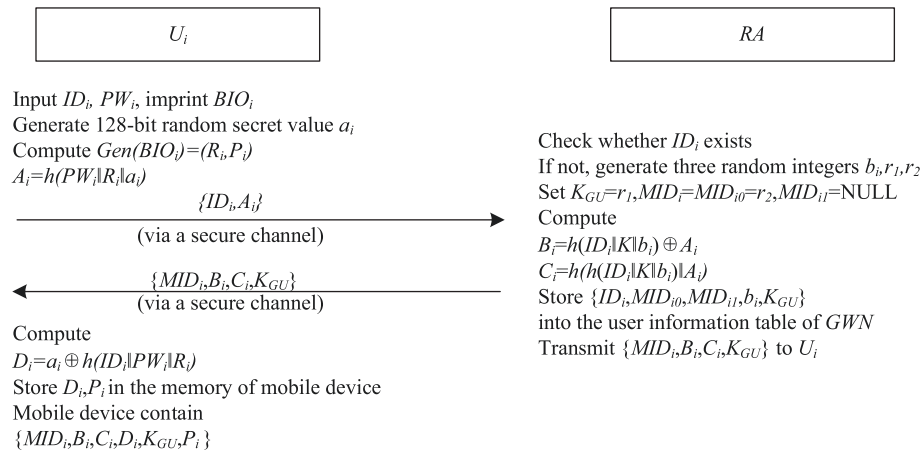

Figure 2: The user registration phase of the proposed scheme.

(i) $\mathcal{A}$ can fully control the open communication channel, i.e., $\mathcal{A}$ can intercept, modify, insert, and delete the transmitted messages over insecure public communication channels easily.

(ii) When the MD of user was stolen or obtained by an attacker $\mathcal{A}$, then the secret values stored in the MD can be revealed by $\mathcal{A}$ using side-channel attacks [28].

(iii) $\mathcal{A}$ is a probabilistic polynomial time attacker. In other words, $\mathcal{A}$ can guess the low-entropy password and identity information within polynomial time.

(iv) $\mathcal{A}$ can get the long-term secret keys when forward secrecy is evaluated.

(v) During the registration phase of authentication scheme, the privileged-insider in GWN being an adversary knows the parameters submitted by the user.

(vi) $\mathcal{A}$ may be a legitimate but malicious user.

(vii) $\mathcal{A}$ may be a legitimate but malicious wearable sensor node.

2.4. Basic Knowledge of Fuzzy Extractor. Fuzzy extractor [29] is capable of extracting the uniformly distributed random key R_i from biometric input BIO_i in an error-tolerant way. If another biometric input BIO_i^* remains reasonably similar to BIO_i, the extracted random key R_i remains unchanged with the help of an auxiliary string P_i. An fuzzy extractor contains two procedures (Gen, Rep).

$Gen(BIO_i) = (R_i, P_i)$. Gen is a probabilistic generation procedure allowing to extract random key R_i and an auxiliary string P_i from biometric input BIO_i.

$R_i^* = Rep(BIO_i^*, P_i)$. Rep is a deterministic reproduction procedure allowing to reproduce random key R_i from any biometric input BIO_i^* close to BIO_i with the help of auxiliary string P_i.

3. The Proposed Scheme

In this section, a lightweight and secure three-factor authentication scheme for remote patient monitoring using oBWNs is presented, which not only withstands all know passive and active attacks, but also achieves more security attributes. The proposed scheme includes five phases, i.e., initialization phase, registration phase, login phase, authentication and key agreement phase, password change phase.

3.1. Initialization Phase. The initialization phase is done by the RA in off-line securely. First of all, RA selects two random numbers GID_j and K as the unique identity and master secret key of the GWN. After that, RA selects a collision-resistant cryptographic hash function $h(\cdot) : \{0,1\}^* \longrightarrow \{0,1\}^l$, where l denotes the bit length of function output (e.g., $l = 160$). For each wearable sensor node SN_k, RA selects an unique identity SID_k and stores it into the memory of SN_k.

3.2. Registration Phase. The registration phase of the proposed scheme contains two parts, i.e., user registration phase and wearable sensor node registration phase.

3.2.1. User Registration Phase. When a new user such as a health professional wants to access the data collected by the wearable sensor node in oBWNs, the user must register in RA firstly. As shown in Figure 2, the procedure of user registration is described as follows:

(1) A new user U_i first chooses an unique identity ID_i, a password PW_i, and imprints his/her biometrics BIO_i to the sensor of mobile device MD. After that, the MD generates the secret biometric key R_i and public parameter P_i using the fuzzy extractor probabilistic generation function $Gen(BIO_i) = (R_i, P_i)$. Then, U_i generates a 128-bit random secret value a_i and computes $A_i = h(PW_i \parallel R_i \parallel a_i)$. Finally, U_i submits $\{ID_i, A_i\}$ to RA via a secure channel.

(2) Upon receipt the registration information, RA first checks whether the identity ID_i exists in the user

information table. If it does, RA rejects the registration request. Otherwise, RA generates three random integers b_i, r_1, and r_2 and sets $K_{GU} = r_1$, $MID_i = MID_{i0} = r_2$, and $MID_{i1} = NULL$. After that, RA computes $B_i = A_i \oplus h(ID_i \| K \| b_i)$ and $C_i = h(h(ID_i \| K \| b_i) \| A_i)$ and stores $\{ID_i, MID_{i0}, MID_{i1}, b_i, K_{GU}\}$ into the user information table. Finally, RA copies the user information table to GWN and transmits the registration reply with information $\{MID_i, B_i, C_i, K_{GU}\}$ to U_i securely.

(3) When receiving the information from RA, U_i computes $D_i = h(ID_i \| PW_i \| R_i) \oplus a_i$. After that, U_i stores D_i and P_i in the memory of MD and finishes the registration. At last, the MD contains the parameters $\{MID_i, B_i, C_i, D_i, K_{GU}, P_i\}$.

3.2.2. Wearable Sensor Node Registration Phase. When a new wearable sensor node SN_k is deployed, it should register in RA.

(1) A new wearable sensor node SN_k sends the identity SID_k to RA via a secure channel.

(2) After receiving the identity SID_k and RA first checks whether SID_k exists in the wearable sensor node information table. If it exists, RA refuses the wearable sensor node registration request. Otherwise, RA generates a random integer K_{GS} and sets the initial sequence numbers $NC_k = NC_{k0} = 0$. Then, RA stores $\{SID_k, K_{GS}, NC_{k0}\}$ into the sensor node information table and copies it to GWN. After that, RA sends the parameters $\{K_{GS}, NC_k\}$ to SN_k via a secure channel.

(3) After receiving the message from RA, SN_k stores $\{K_{GS}, NC_k\}$ into its memory secretly.

3.3. Login Phase. When a user U_i wants to access a wearable sensor node, he/she needs to login in GWN first.

(1) U_i first provides his/her identity ID_i and password PW_i into the interface of the MD. U_i also provides his/her biometrics BIO_i^* to the sensor of MD. After that, MD extracts the biometric key R_i^* with $R_i^* = Rep(BIO_i^*, P_i)$. Then, the MD computes $a_i^* = D_i \oplus h(ID_i \| PW_i \| R_i^*)$, $A_i^* = h(PW_i \| R_i \| a_i^*)$, $h(ID_i \| K \| b_i) = B_i \oplus A_i^*$, and $C_i^* = h(h(ID_i \| K \| b_i) \| A_i^*)$ and compares C_i^* with the stored value C_i. If they are not equal, the MD terminates the session. Otherwise, the MD proceeds to the next step.

(2) After verifying the legitimacy of the user U_i, the MD generates a random number R_1 and gets the current time stamp T_1. After that, the user U_i selects the wearable sensor node SN_k that he/she wants to access, and the MD computes $MS_1 = (R_1 \| SID_k) \oplus h(MID_i \| h(ID_i \| K \| b_i) \| K_{GU})$ and $V_1 = h(ID_i \| R_1 \| h(ID_i \| K \| b_i) \| MID_i \| K_{GU} \| T_1)$. Then U_i sends the login request $\{MID_i, MS_1, V_1, T_1\}$ to GWN through a public channel.

3.4. Authentication and Key Agreement Phase. On receiving the login request from U_i, following steps are performed by U_i, GWN, and a wearable sensor node SN_k to establish a session key SK between U_i and SN_k for future secure communication:

(1) Upon receipt of the login request, GWN first checks the validity of the time stamp. GWN gets the current time T_1^* and compares with the received time T_1. If the matching score $|T_1^* - T_1|$ is beyond a predefined threshold value ΔT, GWN terminates the session. Then, GWN searches whether the pseudo identity MID_i exist in the user information table and operates as follows:

(a) If $MID_i = MID_{i0}$, it demonstrates that the pseudonym identities of U_i and GWN are updated in the previous session. After that, GWN extracts ID_i, b_i, K_{GU}, and MID_{i1} from the user information table corresponding to pseudonym identity MID_i. Then, GWN checks whether the one-time hash chain value K_{GU} is updated.

(i) If $MID_{i1} = NULL$, it means that the hash chain value K_{GU} in GWN side is updated in the previous session. Then, GWN computes $(R_1^* \| SID_k) = MS_1 \oplus h(MID_{i0} \| h(ID_i \| K \| b_i) \| K_{GU})$ and $V_1^* = h(ID_i \| R_1^* \| h(ID_i \| K \| b_i) \| MID_{i0} \| K_{GU} \| T_1)$ and checks whether V_1^* matches with the received V_1. If it does not hold, GWN terminates the session. Otherwise, GWN generates a random pseudonym identity MID_{i0}^* and sets $MID_{i1} = MID_{i0}$; $MID_{i0} = MID_{i0}^*$.

(ii) If $MID_{i1} \neq NULL$, it means that the hash chain value K_{GU} in GWN side is not updated in the previous session. Therefore, the hash chain value should be updated. Then, GWN computes $K_{GU}^* = h(K_{GU})$ and $(R_1^* \| SID_k) = MS_1 \oplus h(MID_{i0} \| h(ID_i \| K \| b_i) \| K_{GU}^*)$ and $V_1^* = h(ID_i \| R_1^* \| h(ID_i \| K \| b_i) \| MID_{i0} \| K_{GU}^* \| T_1)$ and checks whether V_1^* matches with the received value V_1. If it does not hold, GWN terminates the session. Otherwise, GWN generates a new random pseudonym identity MID_{i0}^* and sets $MID_{i1} = MID_{i0}$, $MID_{i0} = MID_{i0}^*$, and $K_{GU} = K_{GU}^*$.

(b) If $MID_i = MID_{i1}$, it demonstrates that the pseudonym identity of the user and the hash chain value are not updated in the previous session. Then, GWN extracts the corresponding secret values ID_i, b_i, and K_{GU} and computes $(R_1^* \| SID_k) = MS_1 \oplus h(MID_{i1} \| h(ID_i \| K \| b_i) \| K_{GU})$ and $V_1^* = h(ID_i \| R_1^* \| h(ID_i \| K \| b_i) \| MID_{i1} \| K_{GU} \| T_1)$. Thereafter, GWN compares $V_1^* ? = V_1$. If it holds, GWN generates a random pseudonym identity MID_{i0}^* and sets

$MID_{i0} = MID_{i0}^*$. Otherwise, *GWN* terminates the session.

(c) If $MID_i \neq MID_{i0}$ and $MID_i \neq MID_{i1}$, *GWN* terminates the session directly.

(2) After that, the gateway node *GWN* generates a random number R_2 of 128-bit and computes $MS_2 = (R_1 \| R_2 \| ID_i \| GID_j) \oplus h(K_{GS} \| SID_k \| NC_{k0})$ and $V_2 = h(ID_i \| GID_j \| R_1 \| R_2 \| K_{GS} \| NC_{k0})$. Then, *GWN* updates K_{GS} and NC_{k0} with $K_{GS} = h(K_{GS} \| SID_k)$ and $NC_{k0} = NC_{k0} + 1$, respectively. Finally, *GWN* transmits the message $\{MS_2, V_2, NC_{k0}\}$ to the wearable sensor node SN_k via open channel.

(3) After receiving the message from *GWN*, SN_k first checks whether $1 \leq NC_{k0} - NC_k \leq N$. In the latter inequality, the parameter N is a threshold which sets according to specific application environment. If the inequality does not hold, SN_k terminates the session. Otherwise, SN_k sets $K_{GS}^* = K_{GS}$ and computes $N - 1$ times $K_{GS}^* = h(K_{GS}^* \| SID_k)$. It is noted that if N satisfies $N - 1 = 0$, the above hash operation will not be executed. Then, SN_k computes $(R_1 \| R_2 \| ID_i \| GID_j) = MS_2 \oplus h(K_{GS}^* \| SID_k \| (NC_{k0} - 1))$ and $V_2^* = h(ID_i \| GID_j \| R_1 \| R_2 \| K_{GS}^* \| (NC_{k0} - 1)))$ and compares V_2^* with the received value V_2. If it is satisfied, SN_k updates K_{GS} and NC_{k0} with $K_{GS} = h(K_{GS}^* \| SID_k)$ and $NC_k = NC_{k0}$, respectively. After that, SN_k generates a random number R_3 and computes $SK = h(ID_i \| GID_j \| SID_k \| R_1 \| R_2 \| R_3)$, $MS_3 = R_3 \oplus h(K_{GS} \| SID_k \| NC_k)$, and $V_3 = h(SID_k \| ID_i \| SK \| R_3 \| NC_k)$. At last, the wearable sensor node SN_k sends the message $\{MS_3, V_3\}$ to *GWN* through a public channel.

(4) After getting the message from SN_k, the gateway node *GWN* computes $R_3^* = MS_3 \oplus h(K_{GS} \| SID_k \| NC_{k0})$, $SK = h(ID_i \| GID_j \| SID_k \| R_1 \| R_2 \| R_3^*)$, and $V_3^* = h(SID_k \| ID_i \| SK \| R_3^* \| NC_{k0})$. Then, *GWN* checks whether V_3^* matches with V_3. If it is failed, *GWN* terminates the session. Otherwise, *GWN* computes $MS_4 = (R_2 \| R_3 \| GID_j \| MID_{i0}) \oplus h(R_1 \| h(ID_i \| K \| b_i) \| K_{GU} \| MID_{i1})$ and $V_4 = h(ID_i \| SID_k \| SK \| R_2 \| MID_{i0})$. Finally, *GWN* sends the message $\{MS_4, V_4\}$ to U_i through a public channel.

(5) After receiving the message, U_i computes $(R_2 \| R_3 \| GID_j \| MID_{i0}) = MS_4 \oplus h(R_1 \| h(ID_i \| K \| b_i) \| K_{GU} \| MID_i)$, $SK = h(ID_i \| GID_j \| SID_k \| R_1 \| R_2 \| R_3)$, and $V_4^* = h(ID_i \| SID_k \| SK \| R_2 \| MID_{i0})$. After that, U_i checks whether V_4^* matches with the received value V_4. If it does not hold, U_i terminates the session. Otherwise, U_i computes $V_5 = h(ID_i \| GID_j \| SID_k \| MID_{i0} \| SK)$ and updates K_{GU} and MID_i with $K_{GU} = h(K_{GU})$ and $MID_i = MID_{i0}$, respectively. Then, U_i sends the message $\{V_5\}$ to *GWN* through a public channel.

(6) After receiving $\{V_5\}$, *GWN* computes $V_5^* = h(ID_i \| GID_j \| SID_k \| MID_{i0} \| SK)$ and checks whether V_5^* matches with the received value V_5. If it does not hold, *GWN* terminates the session. Otherwise, *GWN* updates K_{GU} and MID_{i1} with $K_{GU} = h(K_{GU})$ and $MID_{i1} = NULL$, respectively. Then, a symmetric session key SK is established between the user and the wearable sensor node for future secure communications.

The procedure of login, authentication, and key agreement phases are summarized in Figure 3.

3.5. Password Change Phase. In this phase, U_i can change his/her password without contacting the *RA*. For this purpose, he/she must perform the following steps:

(1) U_i first provides his/her identity ID_i and password PW_i into the interface of the *MD*. After that, U_i also provides his/her biometrics BIO_i^* to the sensor of *MD*. Then, the *MD* computes R_i^* with $R_i^* = Rep(BIO_i^*, P_i)$, $a_i^* = D_i \oplus h(ID_i \| PW_i \| R_i^*)$, $A_i^* = h(PW_i \| R_i \| a_i^*)$, $h(ID_i \| K \| b_i) = B_i \oplus A_i^*$, and $C_i^* = h(h(ID_i \| K \| b_i) \| A_i^*)$. *MD* compares C_i^* with the stored value C_i. If they are not equal, the *MD* rejects the password change request. Otherwise, the *MD* believes the legitimacy of the user and allows U_i to input a new password PW_i^{new}.

(2) The *MD* computes $A_i^{new} = h(PW_i^{new} \| R_i \| a_i)$, $B_i^{new} = h(ID_i \| K \| b_i) \oplus A_i^{new} = B_i \oplus A_i \oplus A_i^{new}$, and $C_i^{new} = h(h(ID_i \| K \| b_i) \| A_i^{new})$.

(3) At last, B_i^{new} and C_i^{new} are stored in the *MD* to replace B_i and C_i, respectively.

4. Security Analysis

In this section, the security of the proposed scheme has been analyzed. First of all, we conduct a formal security analysis using BAN logic [25] to demonstrate that the proposed scheme achieves mutual authentication successfully. After that, we indicate that the proposed scheme can resist all known attacks and provide the desired security features.

4.1. Formal Security Analysis Using BAN Logic. BAN logic is a set of rules for defining and analyzing authentication protocols, which is widely used in many works, such as the schemes in [5, 6, 30, 31]. For convenience, all the notations used in the BAN logic are given in Table 2:

Basic rules of BAN logic are given in Table 3.

The proposed scheme should accomplish the following four goals:

Goal1: $U_i| \equiv (U_i \overset{SK}{\longleftrightarrow} SN_k)$

Goal2: $U_i| \equiv SN_k| \equiv (U_i \overset{SK}{\longleftrightarrow} SN_k)$

Goal3: $SN_k| \equiv (U_i \overset{SK}{\longleftrightarrow} SN_k)$

Goal4: $SN_k| \equiv U_i| \equiv (U_i \overset{SK}{\longleftrightarrow} SN_k)$

First, the messages exchanged in the proposed scheme can be transformed into idealized forms as follows:

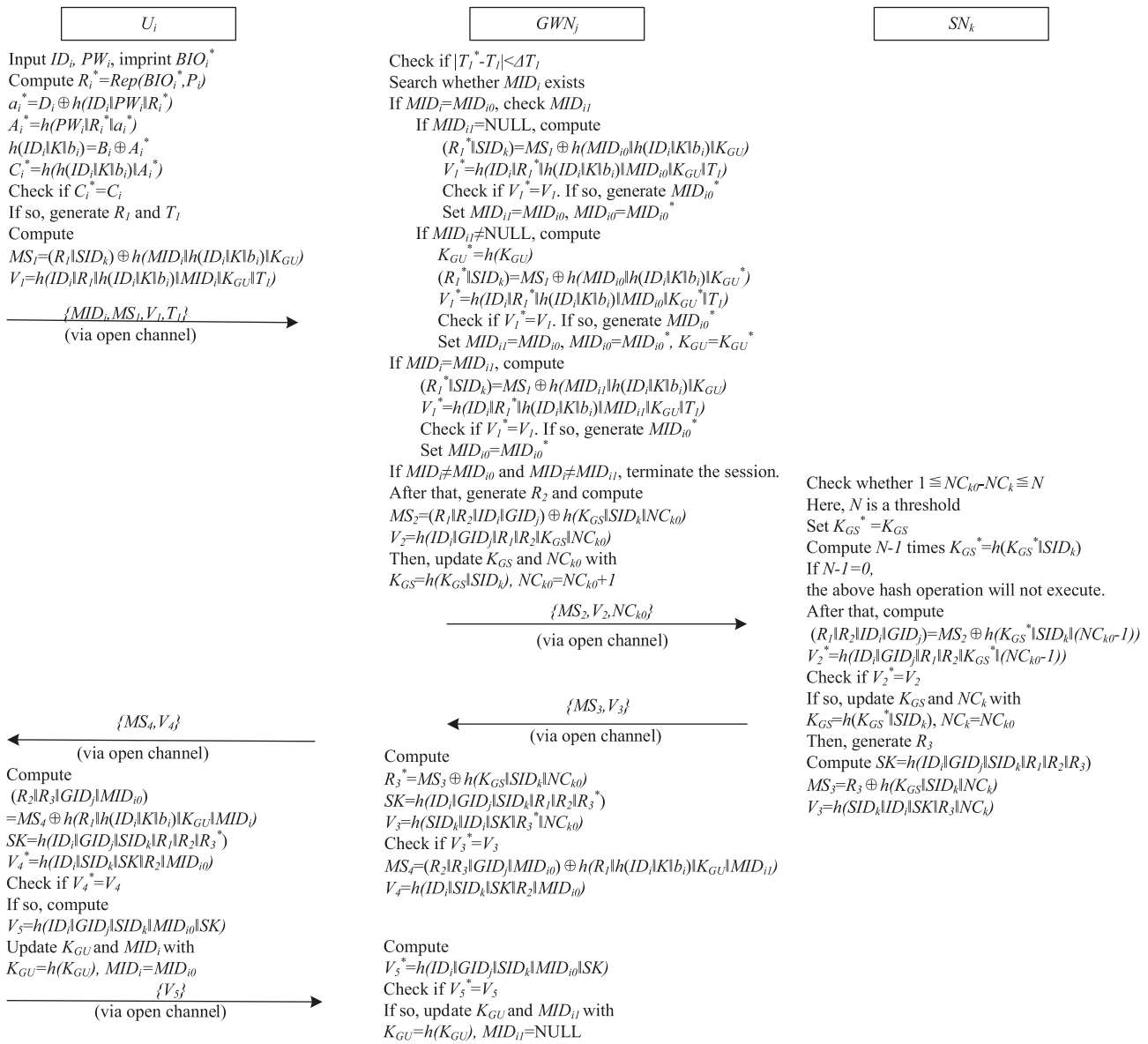

Figure 3: Login, authentication, and key agreement phase of the proposed scheme.

Msg1: $U_i \longrightarrow GWN_j$:

$< ID_i, R_1, MID_i, SID_k, T_1, U_i \overset{h(ID_i\|K\|b_i)}{\longleftrightarrow} GWN_j >_{U_i \overset{K_{GU}}{\longleftrightarrow} GWN_j}$

Msg2: $GWN_j \longrightarrow SN_k$:

$< ID_i, GID_j, SID_k, R_1, R_2, NC_{k0} >_{GWN_j \overset{K_{GS}}{\longleftrightarrow} SN_k}$

Msg3: $SN_k \longrightarrow GWN_j$:

$< ID_i, SID_k, R_3 >_{SN_k \overset{K_{GS}}{\longleftrightarrow} GWN_j}$

Msg4: $GWN_j \longrightarrow U_i$:

$< ID_i, GID_j, SID_k, MID_i, R_1, R_2, R_3, GWN_j \overset{h(ID_i\|K\|b_i)}{\longleftrightarrow} U_i >_{GWN_j \overset{K_{GU}}{\longleftrightarrow} U_i}$

Msg5: $U_i \longrightarrow GWN_j$:

$< ID_i, GID_j, SID_k, MID_i, R_1, R_2, R_3, U_i \overset{h(ID_i\|K\|b_i)}{\longleftrightarrow} GWN_j >_{U_i \overset{K_{GU}}{\longleftrightarrow} GWN_j}$

Second, some initial assumptions about the proposed scheme are listed below:

A1: $GWN_j| \equiv \#(T_1)$

A2: $GWN_j| \equiv \#(R_1, R_2, R_3)$

A3: $SN_k| \equiv \#(R_1, R_2, R_3)$

A4: $U_i| \equiv \#(R_1, R_2, R_3)$

A5: $U_i| \equiv U_i \overset{K_{GU}}{\longleftrightarrow} GWN_j$

A6: $GWN_j| \equiv U_i \overset{K_{GU}}{\longleftrightarrow} GWN_j$

Table 2: Notations in BAN logic.

Notation	Implications
$P \triangleleft X$	Principal P sees a statement X
$P\vert \equiv X$	Principal P believes a statement X
$P\vert \Longrightarrow X$	Principal P has jurisdiction over statement X
$P\vert \sim X$	Principal P once said a statement X
$\#(X)$	Statement X is fresh
(X, Y)	Statement X or Y is one part of statement (X, Y)
X_K	Statement X is encrypted with the key K
$< X >_Y$	Statement X is combined with statement Y
$(X)_K$	Statement X is hashed with the key K
$P \overset{K}{\longleftrightarrow} Q$	Principal P and principal Q communicate with the shared key K

Table 3: Basic rules of BAN logic.

Rule	Description
Message-meaning rule	$\dfrac{P\vert \equiv P \overset{K}{\longleftrightarrow} Q, P \triangleleft X_K}{P\vert \equiv Q\vert \sim X}$
Nonce-verification rule	$\dfrac{P\vert \equiv \#(X), P\vert \equiv Q\vert \sim X}{P\vert \equiv Q\vert \equiv X}$
Jurisdiction rule	$\dfrac{P\vert \equiv Q\vert \Longrightarrow X, P\vert \equiv Q\vert \equiv X}{P\vert \equiv X}$
Freshness rule	$\dfrac{P\vert \equiv \#(X)}{P\vert \equiv \#(X, Y)}$

A7: $SN_k\vert \equiv SN_k \overset{K_{GS}}{\longleftrightarrow} GWN_j$

A8: $GWN_j\vert \equiv SN_k \overset{K_{GS}}{\longleftrightarrow} GWN_j$

A9: $U_i\vert \equiv SN_k\vert \Longrightarrow U_i \overset{SK}{\longleftrightarrow} SN_k$

A10: $SN_k\vert \equiv U_i\vert \Longrightarrow U_i \overset{SK}{\longleftrightarrow} SN_k$

Third, based on the BAN logic rules and assumptions, the main proofs are performed as follows.

According to the Msg1, we get

S1: $GWN_j \triangleleft< ID_i, R_1, MID_i, SID_k, T_1, U_i \overset{h(ID_i\|K\|b_i)}{\longleftrightarrow} GWN_j >_{U_i \overset{K_{GU}}{\longleftrightarrow} GWN_j}$

Based on Assumption A6, S1, and message-meaning rule, we have

S2: $GWN_j\vert \equiv U_i\vert \sim (ID_i, R_1, MID_i, SID_k, T_1, U_i \overset{h(ID_i\|K\|b_i)}{\longleftrightarrow} GWN_j)$

From A1, A2, and freshness rule, we get

S3: $GWN_j\vert \equiv \#(ID_i, R_1, MID_i, SID_k, T_1, U_i \overset{h(ID_i\|K\|b_i)}{\longleftrightarrow} GWN_j)$

From S3, S2, and nonce-verification rule, we get

S4: $GWN_j\vert \equiv U_i\vert \equiv (ID_i, R_1, MID_i, SID_k, T_1, U_i \overset{h(ID_i\|K\|b_i)}{\longleftrightarrow} GWN_j)$

According to the Msg2, we get

S5: $SN_k \triangleleft< ID_i, GID_j, SID_k, R_1, R_2, NC_{k0} >_{GWN_j \overset{K_{GS}}{\longleftrightarrow} SN_k}$

From A7, S5, and message-meaning rule, we have

S6: $SN_k\vert \equiv GWN_j\vert \sim (ID_i, GID_j, SID_k, R_1, R_2, NC_{k0})$

From A3 and freshness rule, we get

S7: $SN_k\vert \equiv \#(ID_i, GID_j, SID_k, R_1, R_2, NC_{k0})$

From S7, S6, and nonce-verification rule, we get

S8: $SN_k\vert \equiv GWN_j\vert \equiv (ID_i, GID_j, SID_k, R_1, R_2, NC_{k0})$

According to the Msg3, we get

S9: $GWN_j \triangleleft< ID_i, SID_k, R_3 >_{SN_k \overset{K_{GS}}{\longleftrightarrow} GWN_j}$

From A8, S9, and message-meaning rule, we have

S10: $GWN_j\vert \equiv SN_k\vert \sim (ID_i, SID_k, R_3)$

From A2 and freshness rule, we get

S11: $GWN_j\vert \equiv \#(ID_i, SID_k, R_3)$

From S11, S10, and nonce-verification rule, we get

S12: $GWN_j\vert \equiv SN_k\vert \equiv (ID_i, SID_k, R_3)$

According to the Msg4, we get

S13: $U_i \triangleleft< ID_i, GID_j, SID_k, MID_i, R_1, R_2, R_3, GWN_j \overset{h(ID_i\|K\|b_i)}{\longleftrightarrow} U_i >_{GWN_j \overset{K_{GU}}{\longleftrightarrow} U_i}$

From A5, S13, and message-meaning rule, we have

S14: $U_i\vert \equiv GWN_j\vert \sim (ID_i, GID_j, SID_k, MID_i, R_1, R_2, R_3, GWN_j \overset{h(ID_i\|K\|b_i)}{\longleftrightarrow} U_i)$

From A4 and freshness rule, we get

S15: $U_i\vert \equiv \#(ID_i, GID_j, SID_k, MID_i, R_1, R_2, R_3, GWN_j \overset{h(ID_i\|K\|b_i)}{\longleftrightarrow} U_i)$

From S15, S14, and nonce-verification rule, we get

S16: $U_i\vert \equiv GWN_j\vert \equiv (ID_i, GID_j, SID_k, MID_i, R_1, R_2, R_3, GWN_j \overset{h(ID_i\|K\|b_i)}{\longleftrightarrow} U_i)$

According to the Msg5, we get

S17: $GWN_j \triangleleft< ID_i, GID_j, SID_k, MID_i, R_1, R_2, R_3, U_i \overset{h(ID_i\|K\|b_i)}{\longleftrightarrow} GWN_j >_{U_i \overset{K_{GU}}{\longleftrightarrow} GWN_j}$

From A6, S17, and message-meaning rule, we have

S18: $GWN_j\vert \equiv U_i\vert \sim (ID_i, GID_j, SID_k, MID_i, R_1, R_2, R_3, U_i \overset{h(ID_i\|K\|b_i)}{\longleftrightarrow} GWN_j)$

From A2 and freshness rule, we get

S19: $GWN_j\vert \equiv \#(ID_i, GID_j, SID_k, MID_i, R_1, R_2, R_3, U_i \overset{h(ID_i\|K\|b_i)}{\longleftrightarrow} GWN_j)$

From S18, S19, and nonce-verification rule, we get

S20: $GWN_j\vert \equiv U_i\vert \equiv (ID_i, GID_j, SID_k, MID_i, R_1, R_2, R_3, U_i \overset{h(ID_i\|K\|b_i)}{\longleftrightarrow} GWN_j)$

From S12, S16, and $SK = h(ID_i \parallel GID_j \parallel SID_k \parallel R_1 \parallel R_2 \parallel R_3)$, we have

S21: $U_i| \equiv SN_k| \equiv (U_i \overset{SK}{\longleftrightarrow} SN_k)$ (Goal2)

From S4, S8, S20, and $SK = h(ID_i \parallel GID_j \parallel SID_k \parallel R_1 \parallel R_2 \parallel R_3)$, we have

S22: $SN_k| \equiv U_i| \equiv (U_i \overset{SK}{\longleftrightarrow} SN_k)$ (Goal4)

From S21, A9, and jurisdiction rule, we have

S23: $U_i| \equiv (U_i \overset{SK}{\longleftrightarrow} SN_k)$ (Goal1)

From S22, A10, and jurisdiction rule, we have

S24: $SN_k| \equiv (U_i \overset{SK}{\longleftrightarrow} SN_k)$ (Goal3)

Therefore, the security of the proposed scheme is proved strictly. In other words, the proposed scheme can achieve mutual authentication successfully.

4.2. Further Security Analysis of the Proposed Scheme. In this section, the security and functional features of the proposed scheme are discussed.

4.2.1. Mutual Authentication. In the execution of the proposed scheme, the users U_i and GWN_j authenticate each other by checking V_1, V_4, and V_5, respectively. Similarly, GWN_j and the wearable sensor node SN_k authenticate each other by checking V_2 and V_3, respectively. In addition, as demonstrated in Section 4.1, the security of the proposed scheme has been proved strictly based on the BAN logic. Therefore, the proposed scheme achieves mutual authentication successfully.

4.2.2. Session Key Agreement. After mutual authentication has been achieved successfully, a shared session key $SK = h(ID_i \parallel GID_j \parallel SID_k \parallel R_1 \parallel R_2 \parallel R_3)$ is established between the user U_i and the wearable sensor node SN_k to protect future communications. The session key SK contains U_i's contribution ID_i, R_1, GWN_j's contribution GID_j, R_2, and SN_k's contribution SID_k, R_3. Any third party can not predetermine the session key. Therefore, the proposed scheme provides session key agreement.

4.2.3. User Anonymity. In the proposed scheme, pseudonym identity technique is adopted to protect the real identity of the user. In particular, a pseudonym identity MID_i, instead of the user's real identity ID_i, is generated randomly and sent to GWN. In order to resist tracking attack, the pseudonym identity MID_i is updated after every session. Since one-way hash function is used, it is almost impossible to get the real identity of the user if the transmitted messages are intercepted by an adversary. To be more important, the transmitted messages in current session are also different from other sessions. Therefore, the proposed scheme can provide user anonymity and untraceability.

4.2.4. Forward Secrecy. Forward secrecy means that the encrypted communications and session keys in the past cannot be retrieved and decrypted even if the long-term secret keys are compromised. In the proposed scheme, if the long-term keys K_{GU} and K_{GS} are compromised by an attacker, the confidentiality of past communications are not affected. The reason is that the long-term keys are updated successfully by one-way hash function after each session. Specifically, the long-term keys K_{GU} and K_{GS} are updated by $K_{GU}^* = h(K_{GU})$ and $K_{GS}^* = h(K_{GS} \parallel SID_k)$, and the attacker can not get K_{GU} and K_{GS} from K_{GU}^* and K_{GS}^*. Therefore, the proposed scheme provides forward secrecy.

4.2.5. Resist Desynchronization Attack. As discussed in Sections 4.2.3 and 4.2.4, pseudonym identity and one-time hash chain techniques are employed to provide user anonymity and forward secrecy in the proposed scheme. However, the incorrect use of pseudonym identity may lead to the problem of desynchronization attack, such as the schemes in [4–6]. In order to ensure the consistency of the pseudonym identity and the value of hash chain, two pseudonym identities MID_{i0} and MID_{i1}, and serial numbers NC_{k0}, NC_k are used, respectively. To perform a comprehensive analysis of this attack, an adversary $\mathcal{A}$ is assumed to launch the following malicious scenarios.

Scenario 1. This scenario indicates that the message $\{MID_i, MS_1, V_1, T_1\}$ has been blocked by an adversary $\mathcal{A}$. However, it is ineffective because all the participants have not even started updating.

Scenario 2. This scenario demonstrates that the message $\{MS_2, V_2, NC_{k0}\}$ has been blocked and the communication between GWN and the wearable sensor node SN_k will be jammed. At this time, the hash chain values of two participants will not match each other. However, the proposed scheme is still usable. The reason is that the proposed scheme uses two serial numbers NC_{k0} and NC_k to record the number of hash chain updated, where NC_{k0} represents the serial number in GWN side and NC_k denotes the serial number in the wearable sensor node side. When the GWN transfers the message $\{MS_2, V_2, NC_{k0}\}$, the hash chain value K_{GS} and sequence number NC_{k0} in GWN side are updated. After receiving the message $\{MS_2, V_2, NC_{k0}\}$, the value of hash chain in SN_k side can be synchronized through performing $NC_{k0} - NC_k$ times hash operations. Therefore, this scenario will not have any impact on the future session.

Scenario 3. If $\mathcal{A}$ blocks the message $\{MS_3, V_3\}$, the desynchronization attack will not work because the hash chain values have been updated and they are equal to each other. Therefore, this scenario will be omitted.

Scenario 4. If the message $\{MS_4, V_4\}$ is blocked, the communication between U_i and GWN will be jammed, and the pseudonym identity values of two participants will not match each other. However, this scenario has no effect on our scheme. In this scenario, both the hash chain values in two participants and the value of pseudonym identity MID_i in the U_i side are not changed, and the value of pseudonym identity MID_{i0} in the GWN side has been a new value generated randomly. Fortunately, the GWN stores

the user's old pseudonym identity in MID_{i1} with $MID_{i1} = MID_i$, and mutual authentication can still be completed successfully even if U_i initiates a new session using unchanged MID_i. Therefore, this scenario may cause the problem of asynchronous, but it will not have any impact on the future session.

Scenario 5. If $\mathcal{A}$ blocks the message $\{V_5\}$, the communication between U_i and *GWN* will be jammed, and the hash chain values of two participants will not match each other. However, this scenario has no effect on our scheme. In this scenario, the values of two participants' pseudonym identities and the hash chain in the U_i side have been updated, but the value of hash chain in the *GWN* side has unchanged. When a new session has been initiated by the U_i using changed hash chain value, the *GWN* will update the hash chain value by checking whether the value of MID_{i1} is nonnull. Therefore, this scenario may cause the problem of asynchronous between U_i and *GWN*, but the two pseudonym identities MID_{i0} and MID_{i1} will make the hash chain values synchronize again.

Therefore, the proposed scheme is resilient to desynchronization attack.

4.2.6. Resist User Impersonation Attack. In the proposed scheme, without knowing the password PW_i, the fingerprint information BIO_i, and the secret key K_{GU}, the adversary is infeasible to forge a legal user and generate a valid message $\{MID_i, MS_1, V_1, T_1\}$. Therefore, the proposed scheme is resilient to user impersonation attack.

4.2.7. Resist Mobile Device Loss Attack. If the *MD* of the user has been stolen or picked up by a malicious user, the stored secret messages $\{MID_i, B_i, C_i, D_i, K_{GU}, P_i\}$ can be revealed using side-channel attacks [28], where $C_i^* = h(h(ID_i \parallel K \parallel b_i) \parallel A_i^*)$, $h(ID_i \parallel K \parallel b_i) = B_i \oplus A_i^*$, $A_i^* = h(PW_i \parallel R_i \parallel a_i^*)$, $a_i^* = D_i \oplus h(ID_i \parallel PW_i \parallel R_i^*)$, and $R_i^* = Rep(BIO_i^*, P_i)$. In addition, as discussed in Section 2.3, the attacker can intercept, modify, insert, and delete the transmitted messages over insecure public communication channels easily. Using this sensitive information, the attacker can launch the mobile device loss attack and try to guess the identity ID_i and password PW_i of the user. However, without knowing the secret random value a_i and biometric input BIO_i of the user, the secret key K, and the high entropy random integer b_i of the *GWN*, the attacker can not obtain the correct identity and password of the user. Therefore, the proposed scheme can resist against mobile device loss attack.

4.2.8. Resist Replay Attack. In the proposed scheme, the time stamp, serial number method, and challenge-response mechanism are used to prevent the replay attack. In detail, the method of using time stamp is used to prevent the replay attack for the first message between U_i and *GWN*, and the rest messages between U_i and *GWN* adopt the challenge-response mechanism. At the same time, the messages between *GWN* and SN_k adopt the serial number method to prevent the replay attack. Therefore, the proposed scheme can resist the replay attack.

4.2.9. Resist Privileged-Insider Attack. In the phase of user registration, U_i sends $\{ID_i, A_i\}$ to *GWN* through a secure channel, where $A_i = h(PW_i \parallel R_i \parallel a_i)$. The three secret values PW_i, R_i, and a_i, generated by U_i, are high entropy random numbers which is unknown to G*WN*. A malicious privileged-insider attacker can not guess the U_i's password PW_i from A_i since it is protected by the one-way hash function. Therefore, the proposed scheme is secure in the privileged-insider attack.

4.2.10. Resist Stolen Verifier Table Attack. In the proposed scheme, the *GWN* maintains the secret values $\{ID_i, MID_{i0}, MID_{i1}, b_i, K_{GU}\}$ for authentication purpose, which has no any password-verifier information of the user. Besides, if an adversary steals the secret values $\{ID_i, MID_{i0}, MID_{i1}, b_i, K_{GU}\}$, he/she still fails to compute $MS_1 = (R_1 \parallel SID_k) \oplus h(MID_i \parallel h(ID_i \parallel K \parallel b_i) \parallel K_{GU})$, $V_1 = h(ID_i \parallel R_1 \parallel h(ID_i \parallel K \parallel b_i) \parallel MID_i \parallel K_{GU} \parallel T_1)$, $h(ID_i \parallel K \parallel b_i) = B_i \oplus A_i$, $A_i = h(PW_i \parallel R_i \parallel a_i)$, $a_i = D_i \oplus h(ID_i \parallel PW_i \parallel R_i)$, and $R_i = Rep(BIO_i, P_i)$ without the knowledge of the user's ID_i, PW_i, and BIO_i and the secret values $\{MID_i, B_i, C_i, D_i, K_{GU}, P_i\}$ in the *MD*. The adversary fails to send the authentication request $\{MID_i, MS_1, V_1, T_1\}$ to *GWN*, and a failure login is detected by *GWN*. Therefore, the proposed scheme can resist stolen verifier table attack.

4.2.11. Quick Detection for Unauthorized Login. Quick detection mechanism for unauthorized login is essential for the authentication scheme. In the phase of user login, the value C_i stored in the mobile device is used to verify the legitimacy of the user U_i, where $C_i^* = h(h(ID_i \parallel K \parallel b_i) \parallel A_i^*)$, $h(ID_i \parallel K \parallel b_i) = B_i \oplus A_i^*$, $A_i^* = h(PW_i \parallel R_i \parallel a_i^*)$, $a_i^* = D_i \oplus h(ID_i \parallel PW_i \parallel R_i^*)$, and $R_i^* = Rep(BIO_i^*, P_i)$. If an attacker inputs the wrong password PW_i^* and the wrong fingerprint information BIO_i, the values C_i^* and C_i are not equal, and the *MD* rejects the U_i's login request. Therefore, the proposed scheme can provide the quick detection mechanism for unauthorized login.

4.3. Security Comparisons. In this subsection, the comparison of security and functional features with six state-of-the-art schemes [4–6, 8, 14, 15] will be described. As shown in Table 4, the six lightweight state-of-the-art schemes fail to provide forward secrecy, and the schemes in [4–6, 14, 15] suffer from the desynchronization attack. In addition, the scheme in [5] is also vulnerable to user impersonation attack, off-line password guessing attack and privileged-insider attack. The scheme in [14] has weaknesses such as sensor node capture attack and privileged-insider attack, and user anonymity is not provided. Besides, the scheme in [15] fails to provide untraceability of the user, and the scheme in [4] lacks the detection mechanism for unauthorized login, and it can lead to unnecessary computational and communication costs. Compared with the state-of-the-art schemes [4–6, 8, 14, 15], the proposed scheme achieves more ideal functional features and resists various malicious attacks.

5. Performance Evaluation

To demonstrate the superiority of the proposed scheme, in this section, six state-of-the-art schemes [4–6, 8, 14, 15] are

Table 4: Security attributes comparison with state-of-the-art schemes.

Schemes	Security attributes										
	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}
Scheme [4]	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Scheme [5]	N	N	Y	N	Y	Y	Y	Y	N	N	N
Scheme [6]	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Scheme [8]	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Scheme [14]	N	N	Y	Y	N	Y	Y	Y	N	Y	Y
Scheme [15]	N	N	Y	Y	N	Y	Y	Y	Y	Y	Y
Our scheme	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Y, yes; N, no; A_1, forward security; A_2, resist desynchronization attack; A_3, mutual authentication; A_4, session key security; A_5, user anonymity; A_6, resist mobile device loss attack; A_7, resist replay attack; A_8, resist wrong password attack; A_9, resist privileged insider attack; A_{10}, resist user impersonation attack; A_{11}, resist off-line password guessing attack.

Table 5: Comparison of computational costs between our scheme and other related schemes.

Scheme	U_i	GWN_j	SN_k	Total cost
Scheme [4]	$11T_h$	$17T_h$	$6T_h$	$34T_h \approx 0.0109s$
Scheme [5]	$12T_h$	$16T_h$	$6T_h$	$34T_h \approx 0.0109s$
Scheme [6]	$2T_{ED} + 11T_h$	$3T_{ED} + 16T_h$	$T_{ED} + 6T_h$	$6T_{ED} + 33T_h \approx 0.0442s$
Scheme [8]	$2T_{ECM} + 10T_h + T_{fe}$	$T_{ECM} + 4T_h$	$5T_h$	$3T_{ECM} + 19T_h + T_{fe} \approx 0.0749s$
Scheme [14]	$T_{fe} + 2T_{ED} + 5T_h$	$6T_{ED} + 6T_h$	$2T_{ED} + 5T_h$	$T_{fe} + 10T_{ED} + 16T_h \approx 0.0782s$
Scheme [15]	$3T_{ED} + 8T_h$	$2T_{ED} + 5T_h$	$2T_{ED} + 5T_h$	$7T_{ED} + 18T_h \approx 0.0449s$
Our scheme	$T_{fe} + 11T_h$	$12T_h$	$7T_h$	$T_{fe} + 30T_h \approx 0.0267s$

selected for comparison. All these schemes are efficient and lightweight, and they are the most representative authentication schemes for remote patient monitoring. In detail, we first compare the computational costs of the proposed scheme with these schemes. Then, the comparisons of communication overheads are presented.

5.1. Computation Analysis. This section will compare the computational efficiency of the proposed scheme with six state-of-the-art schemes [4–6, 8, 14, 15]. We focus only on the login and authentication phase of the proposed scheme, and the costs involved in registration and password change phases are not discussed because these phases are not used frequently. For the convenience of analysis, we define four computational notations T_h, T_{ED}, T_{fe}, and T_{ECM} as the time cost of one-way hash function operation (using SHA-1 hashing algorithm), a general symmetric-key encryption/decryption operation, fuzzy extractor, and an elliptic curve point relative multiplication operation, respectively. The bit *XOR* operation is ignored here because it requires very low computation. According to the experimental results in [32, 33], T_h, T_{ED}, T_{fe}, and T_{ECM} are 0.00032s, 0.0056s, 0.0171s, and 0.0171s, respectively. Table 5 shows the comparison results of computational costs between the proposed scheme and other related schemes.

As shown in Table 5, the total computational cost of the proposed scheme is $T_{fe} + 30T_h \approx 0.0267s$, and it is more efficient than the schemes in [6, 8, 14, 15]. Compared with the schemes in [4, 5], the proposed scheme requires little more computational cost because the fuzzy extractor has been used to provide additional security level of the system. Besides, the proposed scheme provides the desired security features and resists against all the possible attacks.

Table 6: Comparison of communication overheads between our scheme and other schemes.

Scheme	Messages required	Total Bits
Scheme [4]	4 messages	2592 bits
Scheme [5]	4 messages	2272 bits
Scheme [6]	4 messages	2016 bits
Scheme [8]	3 messages	1728 bits
Scheme [14]	4 messages	1312 bits
Scheme [15]	3 messages	1504 bits
our scheme	5 messages	1824 bits

5.2. Communication Analysis. The communication overheads of our schemes and six state-of-the-art schemes [4–6, 8, 14, 15] are compared in Table 6. In order to achieve a convincing comparison, we have made a reasonable assumption that the length of user's identity, user's temporary identity, user's password, sensor node's identity, the time stamp, sequence number, the ECC point multiplication, the secret key, the random number, and the output of hash function are 128 bits, 128 bits, 128 bits, 128 bits, 128 bits, 128 bits, 320 bits, 160 bits, 160 bits, and 160 bits, respectively. In the proposed scheme, the transmitted messages $\{MID_i, MS_1, V_1, T_1\}$, $\{M_2, V_2, NC_{k0}\}$, $\{M_3, V_3\}$, $\{M_4, V_4\}$, and $\{V_5\}$ require (128+160+160+128)=576 bits, (160+160+128)=448 bits,

(160+160)=320 bits, and (160+160)=320 bits and 160 bits, respectively. As a result, the total communication overhead of the proposed scheme is (576+448+320+320+160)=1824 bits. Similarly, the total communication overheads of the schemes in [4–6, 8, 14, 15] are 2592 bits, 2272 bits, 2016 bits, 1728 bits, 1312 bits, and 1504 bits, respectively. From Table 6, it is clear that the proposed scheme is more efficient than Wu et al.'s scheme [4], Amin et al.' scheme [5], and Ali et al.'s scheme [6] in communication overhead. Although the schemes in [8, 15] have slightly advantage in the communication overhead, their schemes are not suitable for realistic environments because the user in their schemes contacts the wearable sensor node directly, and the distance between the user and the wearable sensor node would be higher than the communication radius of sensor node. Besides, the schemes in [4–6, 8, 14, 15] are not secure as they claimed and susceptible to security threats. Therefore, the proposed scheme is more suitable for realistic environments.

6. Conclusion

In this paper, we first briefly review the related authentication schemes for healthcare monitoring, and the security drawbacks of these schemes are pointed out. Specifically, all the schemes using lightweight cryptographic primitives fail to provide forward secrecy and suffer from the desynchronization attack. To overcome the historical security problems, a lightweight and secure three-factor authentication scheme using oBWNs is proposed. The security of the proposed scheme is proved by rigorous formal proof using the BAN logic model. Through the heuristic way, we have proven that the proposed scheme can not only provide some excellent security and functional features, but also resist various malicious attacks, such as desynchronization attack and mobile device loss attack. Comparing with the state-of-the-art schemes, the low computation and communication costs as well as high security make the proposed scheme more suitable for remote patient monitoring in oBWNs-based systems.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

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

[2] L. Wu, Y. Zhang, L. Li, and J. Shen, "Efficient and anonymous authentication scheme for wireless body area networks," *Journal of Medical Systems*, vol. 40, no. 6, pp. 134–146, 2016.

[3] A. Araujo, J. García-Palacios, J. Blesa et al., "Wireless measurement system for structural health monitoring with high time-synchronization accuracy," *IEEE Transactions on Instrumentation and Measurement*, vol. 61, no. 3, pp. 801–810, 2012.

[4] F. Wu, X. Li, A. K. Sangaiah et al., "A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks," *Future Generation Computer Systems*, vol. 82, pp. 727–737, 2017.

[5] R. Amin, S. Islam, G. Biswas, M. Khan, and N. Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," *Future Generation Computer Systems*, vol. 80, pp. 483–495, 2015.

[6] R. Ali, A. K. Pal, S. Kumari, A. K. Sangaiah, X. Li, and F. Wu, "An enhanced three factor based authentication protocol using wireless medical sensor networks for healthcare monitoring," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–22, 2018.

[7] H. Fouchal, J. Biesa, E. Romero, A. Araujo, and O. N. Taladrez, "A security scheme for wireless sensor networks," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM)*, pp. 1–5, 2016.

[8] S. Challa, A. K. Das, V. Odelu et al., "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Computers and Electrical Engineering*, vol. 69, pp. 534–554, 2018.

[9] Q. Jiang, J. Ma, C. Yang, X. Ma, J. Shen, and S. A. Chaudhry, "Efficient end-to-end authentication protocol for wearable health monitoring systems," *Computers and Electrical Engineering*, vol. 63, pp. 182–195, 2017.

[10] P. Kumar, S.-G. Lee, and H.-J. Lee, "E-SAP: efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks," *Sensors*, vol. 12, no. 2, pp. 1625–1647, 2012.

[11] D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, and S.-S. Yeo, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks," *Multimedia Systems*, vol. 21, no. 1, pp. 49–60, 2015.

[12] F. Wu, L. Xu, S. Kumari, and X. Li, "An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks," *Multimedia Systems*, vol. 23, no. 2, pp. 195–205, 2017.

[13] O. Mir, J. Munilla, and S. Kumari, "Efficient anonymous authentication with key agreement protocol for wireless medical sensor networks," *Peer-to-Peer Networking and Applications*, vol. 10, no. 1, pp. 79–91, 2017.

[14] X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, and M. K. Khan, "A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity," *Security and Communication Networks*, vol. 9, no. 15, pp. 2643–2655, 2016.

[15] J. Srinivas, D. Mishra, and S. Mukhopadhyay, "A mutual authentication framework for wireless medical sensor networks," *Journal of Medical Systems*, vol. 41, no. 5, article 80, pp. 80–99, 2017.

[16] A. K. Das, A. K. Sutrala, V. Odelu, and A. Goswami, "A secure smartcard-based anonymous user authentication scheme for healthcare applications using wireless medical sensor networks," *Wireless Personal Communications*, vol. 94, no. 3, pp. 1899–1933, 2017.

[17] P. Chandrakar, "A secure remote user authentication protocol for healthcare monitoring using wireless medical sensor

networks," *International Journal of Ambient Computing and Intelligence*, vol. 10, no. 1, pp. 96–116, 2019.

[18] D. He and S. Zeadally, "Authentication protocol for an ambient assisted living system," *IEEE Communications Magazine*, vol. 53, no. 1, pp. 71–77, 2015.

[19] T. Hayajneh, B. J. Mohd, M. Imran, G. Almashaqbeh, and A. V. Vasilakos, "Secure authentication for remote patient monitoring withwireless medical sensor networks," *Sensors*, vol. 16, no. 4, article 424, pp. 424–449, 2016.

[20] C. H. Liu and Y. F. Chung, "Secure user authentication scheme for wireless healthcare sensor networks," *Computers & Electrical Engineering*, vol. 59, no. 1, pp. 250–261, 2017.

[21] S. Jangirala, A. K. Das, N. Kumar, and J. P. C. Rodrigues, "Cloud centric authentication for wearable healthcare monitoring system," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–14, 2018.

[22] D. Wang, N. Wang, P. Wang, and S. Qing, "Preserving privacy for free: efficient and provably secure two-factor authentication scheme with user anonymity," *Information Sciences*, vol. 321, Article ID 11496, pp. 162–178, 2015.

[23] P. Gope and T. Hwang, "A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 11, pp. 7124–7132, 2016.

[24] L. Xiong, D. Peng, T. Peng, H. Liang, and Z. Liu, "A lightweight anonymous authentication protocol with perfect forward secrecy for wireless sensor networks," *Sensors*, vol. 17, no. 12, pp. 2681–2709, 2017.

[25] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," in *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 426, pp. 233–271, 1989.

[26] M. H. Yang, "Across-authority lightweight ownership transfer protocol," *Electronic Commerce Research and Applications*, vol. 10, no. 4, pp. 375–383, 2011.

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

[28] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology-CRYPTO'99*, vol. 1666 of *Lecture Notes in Computer Science*, pp. 388–397, Springer, Berlin, Germany, 1999.

[29] X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. H. Deng, "A generic framework for three-factor authentication: Preserving security and privacy in distributed systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 8, pp. 1390–1397, 2011.

[30] J. Song, G. Li, B. Xu, and C. Ma, "A novel multiserver authentication protocol with multifactors for cloud service," *Security and Communication Networks*, vol. 2018, pp. 1–13, 2018.

[31] T. Truong, M. Tran, and A. Duong, "Improved chebyshev polynomials-based authentication scheme in client-server environment," *Security and Communication Networks*, vol. 2019, Article ID 4250743, 11 pages, 2019.

[32] C. Lee, C. Chen, P. Wu, and T. Chen, "Three-factor control protocol based on elliptic curve cryptosystem for universal serial bus mass storage devices," *IET Computers & Digital Techniques*, vol. 7, no. 1, pp. 48–55, 2013.

[33] D. B. He, N. Kumar, J. H. Lee, and R. S. Sherratt, "Enhanced three-factor security protocol for USB mass storage devices," *IEEE Transactions on Consumer Electronics*, vol. 60, pp. 30–37, 2014.