Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 5686498, 13 pages
https://doi.org/10.1155/2020/5686498

Research Article

An Improved Anonymous Authentication Protocol for Wearable Health Monitoring Systems

Jiaqing Mo,[1] **Wei Shen**,[1] **and Weisheng Pan**[2]

[1]*School of Computer Science and Software, Zhaoqing University, Zhaoqing, China*
[2]*Education Technology and Computer Center, Zhaoqing University, Zhaoqing, China*

Correspondence should be addressed to Jiaqing Mo; mojiaqing@126.com

Received 1 November 2019; Revised 31 January 2020; Accepted 10 February 2020; Published 23 April 2020

Academic Editor: Antonio Guerrieri

Wearable health monitoring system (WHMS), which helps medical professionals to collect patients' healthcare data and provides diagnosis via mobile devices, has become increasingly popular thanks to the significant advances in the wireless sensor network. Because health data are privacy-related, they should be protected from illegal access when transmitted over a public wireless channel. Recently, Jiang et al. presented a two-factor authentication protocol on quadratic residues with fuzzy verifier for WHMS. However, we observe that their scheme is vulnerable to known session special temporary information (KSSTI) attack, privileged insider attack, and denial-of-service (DoS) attack. To defeat these weaknesses, we propose an improved two-factor authentication and key agreement scheme for WHMS. Through rigorous formal proofs under the random oracle model and comprehensive informal security analysis, we demonstrate that the improved scheme overcomes the disadvantages of Jiang et al.'s protocol and withstands possible known attacks. In addition, comparisons with several relevant protocols show that the proposed scheme achieves more security features and has suitable efficiency. Thus, our scheme is a reasonable authentication solution for WHMS.

1. Introduction

At present, electronic-health (e-health) services are greatly promoted with the significant advances in computer science, wireless communication technologies, low-power sensors, and various security solutions [1–8] have been developed to build secure e-health systems. Wireless sensor network (WSN) plays an important role in e-health via sensing, measuring, gathering patient's information for doctor's diagnosis, or recording in the medical server. Wearable health monitoring system (WHMS), one of the most popular application of e-health notation, has attracted extensive attention in academia and industry for its mobility, flexibility, and low cost [9–12]. WHMS is a WSN, with wearable sensors installed or implanted in the body of the patient, monitors the health conditions of patients by sensing, measuring, and gathering their physiological data and sends them to the medical professional or medical center via a wireless channel for proper diagnosis and further medical treatment. With data like heart rate, blood pressure, and body temperature, doctors in distance can assess the patient's health status. Figure 1 illustrates a typical scenario of WHMS. Advantages of providing healthcare services using WHMS are as follows:

(1) Enhance medical care quality

(2) Continuous monitoring of patients

(3) Save money and time for patients

(4) Real-time physician diagnosis and intervention

1.1. Related Works. Although WHMS provides efficiency and simplicity for medical professionals, and patients can benefit greatly from WHMS, security and privacy cannot be overlooked since the sensed data are transmitted via insecure wireless channels. Thus, it is necessary to design a robust authenticated mechanism to protect the patient's physiological data which are sensitive and should be a secret. If the patient's data are illegally captured and tampered by the attacker, medical professionals will make wrong diagnosis

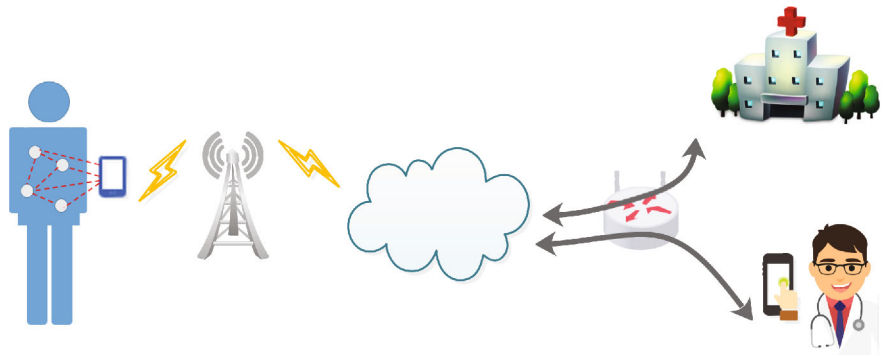

Figure 1: A typical scenario of WHMS.

based on these data. Furthermore, the leaked data may be used for commercial purpose or other horrible purposes. Specifically, medical professionals should be authenticated before accessing the physiological data from the wearable sensors on the patient, and their identity and password should not be revealed if the malicious attacker eavesdrops the messages through the gateway in WHMS, and vice versa. In the meantime, a shared session key should be generated between medical professionals and the sensor node deployed on the patient's body to protect secure communication among the communicating parties.

To address this issue, some user authentication protocols have been proposed for patient's health monitoring [13–23]. Several authentication schemes [16–18] based on elliptical curve cryptography (ECC) have been presented because ECC can reach the identical RSA security level with faster computation and smaller key size. Although the security of these ECC-based schemes are continuously enhanced, these schemes are still not lightweight enough for WHMS since point multiplication consumes a large computation response, while the computation capability and energy of the mobile device and sensors are limited.

Kumar et al. [24] suggested a user authentication protocol named E-SAP to monitor patient's physiological data in wireless medical sensor network in 2012, claiming that their protocol was secure against known attacks. However, both He et al. [25] and Khan and Kumari [26] scrutinized Kumar et al.'s scheme and found some security defects like password guessing attack and lack of user anonymity and put forward their improved versions, respectively. Unfortunately, Wu et al. [20], Mir et al. [21], and Li et al. [22] independently pointed out that He et al.'s scheme [25] was vulnerable to security weaknesses, including denial-of-service attack, impersonation attack, offline guessing attack, and sensor node capture attack. To fix these loopholes, they suggested an improved version and declared that their new proposal was more secure than the previous ones. In 2016, Das et al. [27] identified the security defects in Li et al.'s protocol [28], i.e., privileged insider attack, sensor capture attack, and lack of user anonymity, and suggested an enhanced scheme based on biometrics. Later, Amin et al. [19] introduced a mutual authenticated protocol with user anonymity in WHMS and declared that their scheme was robust against the known threats. However, it was revealed by Jiang et al. [29] that this protocol suffers from several weaknesses, such as stolen mobile device attack, desynchronization attack, and sensor key exposure. To secure Amin et al.'s scheme, Jiang et al. suggested an improved two-factor (password and smartcard) scheme using quadratic residues [29, 30], fuzzy verifier [31], and timestamp mechanism. Further, security analysis showed that their scheme achieved the desired security features; thus, they had confidence in the security of their solution.

Independently, Challa et al. [32] proposed an improved three-factor (password, smartcard, and biometrics) authenticated protocol for wireless healthcare sensor network to improve the security of Liu and Chung's scheme [23]. However, in their scheme the user communicates with the remote sensor directly which means power consumption of the sensor increases greatly, and the sensor's lifetime will reduce rapidly. Thus, their scheme is inapplicable to the wireless healthcare sensor network. Ali et al. [33] devised an anonymous three-factor-based protocol to thwart security threats like offline password guessing attack, user impersonation attack, and known session key temporary information attack in Amin et al.'s scheme [19]. Shen et al. [34] put forward a multilayer authenticated protocol using ECC for the wireless body area network to implement secure authentication and group key generation between the sensor and the mobile device. Li et al. [35] suggested a lightweight authentication protocol for centralized WBAN with two hops while preserving anonymity and unlinkability of data transmission. Shen et al. [36] presented an efficient ECC-based pairing-free certificateless public key signature authentication protocol for WBAN with two round messages. However, according to [37, 38], these kinds of authentication protocol with just two round messages are prone to failure of perfect forward secrecy.

1.2. Motivations and Contributions. When cryptanalyzing Jiang et al.'s scheme [29], regrettably, we find that their protocol is not as robust as they claimed. Although fuzzy verifier is used to thwart offline password guessing attack in Jiang et al.'s scheme, their scheme is still vulnerable to privileged insider attack, which leads to user impersonation attack. Ridiculously, Jiang et al.'s scheme [29] is subject to KSSTI attack, which means that their protocol is vulnerable to sensor key disclosure as the previous one.

Further, we reveal that their protocol suffers from denial-of-service (DoS) attack.

Motivated by the thought of addressing the security defects in Jiang et al.'s scheme [29], we propose an improved two-factor authenticated scheme making use of quadratic residues for WHMS environment.

Our contributions of this work are threefold as listed below:

(i) First, we cryptanalyze the recent authentication scheme of Jiang et al. [29] in WHMS and find its vulnerability of KSSTI attack, privileged insider attack, and DoS attack

(ii) Second, we propose an improved secure two-factor authentication and key agreement using quadratic residues to address the security weaknesses in Jiang et al.'s protocol

(iii) Third, we provide the formal security proof of our proposed scheme under the random oracle model and conduct an informal security analysis to demonstrate that the improved scheme is secure against known attacks. Moreover, we make a performance comparison between the improved protocol and the related schemes

1.3. Organization of the Paper. The remainder of this paper is sketched as follows: Section 2 explains the preliminaries of quadratic residues and security requirements. We cryptanalyze Jiang et al.'s protocol [29] in Section 3. In Section 4, we present our improved two-factor authentication and key agreement scheme for WHMS. Next, security analysis and performance comparison are given in Section 5. Finally, the paper is concluded in Section 6.

2. Preliminaries

2.1. Quadratic Residues. According to [29, 30], the definition of quadratic residue is described as follows.

Let p and q denote two large primes, respectively, and $n = pq$. If there is a solution for $y = x^2 \bmod n$, i.e., y has a square root, then y is called a quadratic residue mod n. Let Q_n be a set of quadratic residue numbers in [1, n-1], and $y \in Q_n$. Because of the difficulty in factoring n, it is hard to find x without the knowledge of p and q.

2.2. Security Requirements. It is important to understand the security requirements in designing or cryptanalyzing an authentication protocol. Hence, according to the previous works [38, 39], the security requirements of authentication protocol for WHMS are summarized as follows.

(1) *Resisting Stolen Mobile Device Attack*. If an unauthorized person obtains the lost/stolen mobile device, it is impossible for him to impersonate a valid user with a counterfeit login request by using the information extracted from the mobile device

(2) *Resisting Impersonation Attack*. The communication parties in WHMS include the user, GWN, and sensor node. It is an important requirement that the attacker is incapable of logging in WHMS to imitate a legitimate user and access the privileged resources in such a way. In addition, if the malicious attacker can impersonate the GWN to identify the legitimacy of the user in the authentication process, it means that the data in sensors can be accessed in an unauthorized manner. The authenticated scheme should also prevent the attacker from sensor node impersonation attack, in which the attacker can impersonate sensor nodes and sends bogus data to the user

(3) *Resisting Known Attacks*. It requires that the authentication scheme for WHMS be secure from various known basic or sophisticated attacks, such as replay attack, privileged insider attack, KSSTI attack, man-in-the-middle attack, and desynchronization attack

(4) *Forward and Backward Secrecy*. It requires that the attacker not be able to obtain the previous session keys or the future ones by using the compromised session key

(5) *User Anonymity*. It is a crucial requirement to prevent the attacker from tracing the user's behavior to preserve user privacy

(6) *Sensor Anonymity*. It is an additional requirement to enhance the security of authentication protocol for WHMS, because the information sent from the sensor to medical professional is sensitive, and sensor anonymity can help confuse the intelligent attacker's traffic analysis that may render the communication ineffective

(7) *Mutual Authentication and Key Agreement*. It is an essential requirement in WHMS scenario, and it requires the communication parties be able to authenticate each other and generate a shared session key to provide confidentiality of messages in wireless channel

3. Cryptanalysis on Jiang et al.'s Protocol

In this section, we cryptanalyze Jiang et al.'s protocol [29]. Due to the space limitation, the review of protocol [29] is omitted. The symbols involved are listed in Table 1.

Jiang et al. [29] criticized Amin et al.'s scheme [19] for its vulnerability of stolen mobile device attack, desynchronization attack, and sensor key exposure. To eliminate these security risks, they put forward countermeasures like public key primitive quadratic residue, the concept of fuzzy verifier, hash function, and timestamp mechanism to enhance the security of Amin et al.'s scheme. Unfortunately, we point out several security vulnerabilities in Jiang et al.'s protocol. More specifically, it is susceptible to KSSTI attack, privileged insider attack, and DoS attack. Before elaborating a security analysis, we summarize the following adversary model used in this work.

Table 1: Notations.

Symbol	Meaning
U_i	Medical professional
GWN	Gateway
S_j	The jth sensor node
MD	The mobile device
ID_i	U_i's identity
PW_i	U_i's password
SID_j	S_j's identity
K	GWN's secret key
R_1, R_2, and R_3	Random nonces produced by U_i, GWN, and S_j, respectively
$h()$	One-way hash function
$\|$	Concatenation
$\oplus$	Bitwise XOR operation

3.1. Adversary Model

(1) The attacker can fully control the open communication channel. In other words, he may eavesdrop, intercept, insert, delete, and modify messages exchanged over an open channel [40, 41]

(2) The attacker can extract all the secret data stored in MD if the lost/stolen mobile device is obtained by him [42, 43]

(3) The attacker can guess the user's identity and password offline by enumerating pairs in (ID and PW) from Cartesian product $D_{\mathrm{ID}} \times D_{\mathrm{PW}}$ in polynomial time, where D_{ID} and D_{PW} denote the identity space and the password space [37, 44], respectively

(4) The random numbers and the secret keys selected by each communication parties are adequately large to prevent the attacker from guessing these data successfully in polynomial time

(5) The insider can obtain the registration request message of the user, and the insider can access the verifier table [45, 46]

3.2. KSSTI Attack. For an authenticated protocol with key agreement, if the attacker cannot compute the session key through the session-specific temporary information such as random number which has been compromised, we say that this protocol is able to resist KSSTI attack. In Jiang et al.'s scheme, if U_i is legitimate, GWN forwards message $\{M_3, M_4, M_5, T_2\}$ to S_j, where $M_4 = M_2 \oplus h(\mathrm{SK}_{\mathrm{GW-}Sj} \| T_2)$, $M_5 = R_2 \oplus \mathrm{h}(\mathrm{SK}_{\mathrm{GW-}Sj} \| T_2)$, and R_2 is a random nonce produced by GWN. After verifying the authenticity of GWN, S_j sends $\{M_6, M_7\}$ to GWN, where $M_7 = h(R_2) \oplus R_3$. If R_2 is compromised and the attacker captures the messages $\{M_3, M_4, M_5, T_2\}$ and $\{M_6, M_7\}$ from the public channel, he can compute the value $h(\mathrm{SK}_{\mathrm{GW-}Sj} \| T_2) = \mathrm{M}_5 \oplus R_2$, $M_2 = M_4 \oplus h(\mathrm{SK}_{\mathrm{GW-}Sj} \| T_2)$, and $R_3 = M_7 \oplus h(R_2)$ and then computes the session key $\mathrm{SK} = \mathrm{h}(M_2 \| R_2 \| R_3)$. Thus, it is not hard to compute the session key if the random number R_2 is disclosed. Therefore, Jiang et al.'s scheme is subject to KSSTI attack.

3.3. Privileged Insider Attack. The similar analysis is mentioned in Das et al. and Das [27, 47]. In the medical professional registration phase, a medical professional U_i sends his registration $\{\mathrm{ID}_i, \mathrm{HPW}_i\}$ to GWN securely, where $\mathrm{HPW}_i = h(r_i \oplus \mathrm{PW}_i)$. Suppose the message $\{\mathrm{ID}_i, \mathrm{HPW}_i\}$ is known by an insider who is being an attacker, and further suppose that the lost/stolen mobile device containing the secret data $(\mathrm{Reg}_i, A_i, C_i, m, n, r_i, h())$ is obtained by the attacker, he can extract all the secret information from the card using side-channel analysis [43]. Note that $A_i = R_i \oplus \mathrm{HPW}_i$, $C_i = B_i \oplus h(\mathrm{ID}_i \oplus R_i \oplus \mathrm{HPW}_i)$. Using these information, the attacker can carry out an attack as follows:

(1) The attacker computes $R_i = A_i \oplus \mathrm{HPW}_i$, $B_i = C_i \oplus h(\mathrm{ID}_i \oplus R_i \oplus \mathrm{HPW}_i)$

(2) The attacker selects a random number $R_1{}'$, and computes $\mathrm{CID}_{\mathrm{i}}' = (\mathrm{ID}_i \| R_{\mathrm{i}}')^2 \bmod n$, $M_1' = h(\mathrm{ID}_i || B_i || R_1' \| T_1)$. T_1 is the current timestamp

(3) The attacker sends $\{\mathrm{SID}_j, \mathrm{CID}_i{}', M_1{}', T_1\}$ to GWN

Upon receipt of the message, GWN will pass the validation to the attacker and treat the attacker as a valid user and successfully perform the subsequent step of the authentication phase as depicted in Jiang et al.'s protocol. Lastly, GWN sends message $\{M_7, M_8, M_9\}$ to the user, but the attacker receives the message and computes $R_2{}' = M_8 \oplus h(\mathrm{ID}_i \| R_1{}')$, $R_3{}' = M_7 \oplus h(R_2{}')$, and $\mathrm{SK}' = h(h(\mathrm{ID}_i \| R_1{}' \| R_2{}') \| R_2{}' \| R_3{}')$ and verifies $M_9{}' ? = h(\mathrm{ID}_i \| \mathrm{SK}' \| R_3{}')$. Obviously, the result is true. Therefore, the attacker has generated a shared session key with S_j.

Thus, the attacker can imitate U_i to login to GWN successfully. In this regard, Jiang et al.'s scheme is not secure against privileged insider attack.

3.4. DoS Attack. To authenticate U_i, GWN maintains a table containing secret data ID_i and R_i with respect to user U_i. When GWN receives the login request from U_i, GWN will retrieve R_i in light of ID_i to perform the subsequent procedure. However, because (ID_i, R_i) is stored in the table, if an insider (being attacker) deletes or modifies all or some entries in the table, GWN will fail to lookup entries related to the user who has successfully registered and sends a login request to GWN, which leads to the legitimate user rejected by the GWN. Therefore, Jiang et al.'s scheme is susceptible to DoS attack.

4. The Proposed Scheme

In this section, we propose a secure and efficient authenticated key agreement scheme for WHMS to thwart the security weaknesses found in Jiang et al.'s scheme. Our scheme not only retains the advantages of Jiang et al.'s scheme but

also provides additional security properties and is secure against different attacks. Similarly, our scheme consists of 5 phases: setup, medical professional registration, patient registration, login and authentication phase, and password change.

4.1. Setup Phase. This phase is identical to that of Jiang et al.'s scheme. The registration center GWN chooses two large prime nonces p and q and calculates $n = pq$, then keeps the private key (p, q).

4.2. Medical Professional Registration Phase

Step 1. U_i keys his ID_i and PW_i, a random nonce r_i, and calculates $\mathrm{HPW}_i = h(r_i \oplus \mathrm{PW}_i)$; then, he transmits $\{\mathrm{ID}_i, \mathrm{HPW}_i\}$ to GWN via a secure channel.

Step 2. Upon receiving the registration request, GWN selects $m \in [2^4, 2^8]$, a random nonce R_i, calculates a fuzzy verifier $\mathrm{Reg}_i = h(h(\mathrm{ID}_i \| R_i \| \mathrm{HPW}_i) \bmod m)$, $A_i = R_i \oplus \mathrm{HPW}_i$, $B_i = h(\mathrm{ID}_i \| R_i \| K)$, and $C_i = B_i \oplus h(\mathrm{ID}_i \| R_i \| \mathrm{HPW}_i)$. After that, GWN sends $\{\mathrm{Reg}_i, A_i, C_i, m, n, h()\}$ to U_i through a secure channel.

Step 3. After receiving the message, U_i calculates $A_i^* = A_i \oplus h(\mathrm{ID}_i \| r_i)$ and $D_i = r_i \oplus h(h(\mathrm{ID}_i \| \mathrm{PW}_i) \bmod m)$ and updates MD with $\{\mathrm{Reg}_i, A_i^*, C_i, D_i, m, n, h()\}$.

4.3. Patient Registration Phase. This phase is almost the same as in Jiang et al.'s scheme [29].

Step 1: The patient forwards his ID to the registration center.

Step 2: The registration center selects an appropriate sensor kit and assigns a professional.

Step 3: The registration center computes $\mathrm{SK}_{\mathrm{GW}-Sj} = h(\mathrm{SID}_j \| K)$ for S_j as secret key and delivers the relevant information of the patient to the designated professional.

4.4. Login and Authentication Phase. In this phase, a mutual authentication is performed and a session key is generated between U_i and sensor S_j for subsequent communication.

Step 1. U_i selects his ID_i and PW_i, and MD computes $r_i = D_i \oplus h(h(\mathrm{ID}_i \| \mathrm{PW}_i) \bmod m)$, $\mathrm{HPW}_i = h(r_i \oplus \mathrm{PW}_i)$, $A_i = A_i^* \oplus h(\mathrm{ID}_i \| r_i)$, $R_i^* = A_i \oplus \mathrm{HPW}_i$, $\mathrm{Reg}_i^* = h(h(\mathrm{ID}_i \| R_i^* \| \mathrm{HPW}_i^*) \bmod m)$, and tests $\mathrm{Reg}_i^* ?= \mathrm{Reg}_i$. If it is false, MD chooses a random number R_1 and computes $B_i^* = C_i \oplus h(\mathrm{ID}_i \| R_i \| \mathrm{HPW}_i)$, $\mathrm{CID}_i = (\mathrm{ID}_i \| R_1 \| R_i^* \| \mathrm{SID}_j)^2 \bmod n$, $M_1 = h(\mathrm{ID}_i \| B_i^* \| R_1 \| T_1)$, then forwards $\mathrm{msg}_1 = \{\mathrm{CID}_i, M_1, T_1\}$ to GWN. T_1 is the current timestamp.

Step 2. On receiving login request msg_1, GWN decrypts CID_i with (p, q) to obtain $(\mathrm{ID}_i^*, R_i^*, R_1^*, T_1)$ and checks the validity of the timestamp T_1. If the verification fails, GWN aborts the session. Otherwise, GWN computes $B_i' = h(\mathrm{ID}_i \| R_i \| K)$ and $M_1^* = h(\mathrm{ID}_i \| B_i' \| R_1 \| T_1)$ and then tests $M_1^* = M_1$. If inequality holds, GWN aborts the procedure. Otherwise, GWN calculates $\mathrm{SK}_{\mathrm{GW}-Sj} = h(\mathrm{SID}_j \| K)$, selects a random nonce R_2, and computes $M_2 = h(\mathrm{ID}_i^* \| R_1^* \| R_i)$, $M_3 = h(h(M_2 \| \text{“1”}) \| \mathrm{SK}_{\mathrm{GW}-Sj} \| R_2 \| T_2)$, $M_4 = M_2 \oplus h(\mathrm{SK}_{\mathrm{GW}-Sj} \| T_2)$, and $M_5 = R_2 \oplus (\mathrm{SK}_{\mathrm{GW}-Sj} \| \mathrm{SID}_j \| T_2)$. Finally, GWN sends $\mathrm{msg}_2 = \{M_3, M_4, M_5, T_2\}$ to S_j.

Step 3. On receiving msg_2 from GWN, S_j first checks the freshness of T_2. If not, S_j terminates the procedure. Otherwise, S_j computes $R_2' = M_5 \oplus (\mathrm{SK}_{\mathrm{GW}-Sj} \| \mathrm{SID}_j \| T_2)$ and $M_2 = M_4 \oplus h(\mathrm{SK}_{\mathrm{GW}-Sj} \| T_2)$ and tests $M_3 ?= h(h(M_2 \| \text{“1”}) \| \mathrm{SK}_{\mathrm{GW}-Sj} \| R_2' \| T_2)$. If it is false, S_j aborts the session. Otherwise, S_j chooses a random number R_3 and computes $\mathrm{SK} = h(M_2' \| R_2' \| R_3)$, $M_6 = h(\mathrm{SK} \| R_3 \| \mathrm{SK}_{\mathrm{GW}-Sj})$, and $M_7 = h(R_2' \| T_3) \oplus R_3$, where T_3 is the current timestamp. S_j then forwards $\mathrm{msg}_3 = \{M_6, M_7, T_3\}$ to GWN.

Step 4. On receiving msg_3 from S_j, GWN first checks the validity of T_3. If it is invalid, GWN terminates the procedure. Otherwise, GWN computes $R_3' = M_7 \oplus h(R_2' \| T_3)$, $\mathrm{SK}' = h(M_2 \| R_2 \| R_3')$, and $M_6' = h(\mathrm{SK}' \| R_3' \| \mathrm{SK}_{\mathrm{GW}-Sj})$ and checks whether $M_6' = M_6$ holds. If yes, GWN computes $M_8 = R_2 \oplus h(\mathrm{ID}_i^* \| R_1^*)$, $M_9 = R_3 \oplus h(\mathrm{ID}_i^* \| R_2^*)$, and $M_{10} = h(\mathrm{ID}_i^* \| \mathrm{SK}' \| R_3 \| T_4)$ and delivers $\mathrm{msg}_4 = \{M_8, M_9, M_{10}, T_4\}$ to U_i, where T_4 is the current timestamp.

Step 5. After receiving msg_4 from GWN, U_i validates the timestamp T_4. If not, U_i aborts the procedure. Otherwise, U_i computes $R_2' = M_8 \oplus h(\mathrm{ID}_i \| R_1)$, $R_3' = M_9 \oplus h(\mathrm{ID}_i \| R_2')$, and $\mathrm{SK}^* = h(h(\mathrm{ID}_i \| R_1 \| R_i') \| R_2' \| R_3')$ and checks whether $M_{10} ?= h(\mathrm{ID}_i \| \mathrm{SK}^* \| R_3' \| T_4)$ holds. If it is false, U_i terminates the connection. Otherwise, U_i believes that both GWN and S_j are credible.

The login and authentication phase is summarized in Figure 2.

4.5. Password Change Phase. This phase is also similar to that in Jiang et al.'s scheme [29], and it is applicable if U_i intends to update his password.

Step 1. U_i keys ID_i and PW_i.

Step 2. MD computes $\mathrm{HPW}_i^* = h(r_i \oplus \mathrm{PW}_i)$, $A_i = A_i^* \oplus h(\mathrm{ID}_i \| r_i)$, $R_i^* = A_i \oplus \mathrm{HPW}_i^*$, and $\mathrm{Reg}_i^* = h(h(\mathrm{ID}_i \| R_i^* \| \mathrm{HPW}_i^*) \bmod m)$ and checks the condition $\mathrm{Reg}_i^* = \mathrm{Reg}_i$. If it holds, MD quits this procedure.

Step 3. U_i keys his new password $\mathrm{PW}_i^{\mathrm{new}}$; then, MD computes $\mathrm{HPW}_i^{\mathrm{new}} = h(r_i \oplus \mathrm{PW}_i^{\mathrm{new}})$, $\mathrm{Reg}_i^{\mathrm{new}} = h(h(\mathrm{ID}_i \| R_i \| \mathrm{HPW}_i^{\mathrm{new}}) \bmod m)$, $A_i^{\mathrm{new}} = R_i^{\mathrm{new}} \oplus \mathrm{HPW}_i^{\mathrm{new}}$, $B_i = C_i \oplus h(\mathrm{ID}_i \| R_i \| \mathrm{HPW}_i)$, $C_i^{\mathrm{new}} = B_i \oplus h(\mathrm{ID}_i \| R_i^* \| \mathrm{HPW}_i^{\mathrm{new}})$, and $A_i^{*\mathrm{new}} = A_i^{\mathrm{new}} \oplus h(\mathrm{ID}_i \| r_i)$.

Step 4. Finally, $(\mathrm{Reg}_i, A_i^*, C_i)$ is replaced with $(\mathrm{Reg}_i^{\mathrm{new}}, A_i^{*\mathrm{new}}, C_i^{\mathrm{new}})$ by MD.

U_i/mobile device	GWN	S_j
Input <ID_i, PW_i>; $r_i = D_i \oplus h(h(ID_i \| PW_i) \bmod m)$; $HPW_i = h(r_i \oplus PWi)$; $A_i = A_i^* \oplus h(ID_i \| r_i)$; $R_i^* = A_i \oplus HPW_i$; $Reg_i^* = h(h(ID_i \| R_i^* \| HPW_i^*) \bmod m)$; If $Reg_i^* \neq Reg_i^*$, abort; Choose R_1; $B_i^* = C_i \oplus h(ID_i \| R_i \| HPW_i)$; $CID_i = (ID_i \| R_1 \| R_i^* \| SID_j)^2 \bmod n$; $M_1 = h(ID_i \| B_i^* \| R_1 \| T_1)$; $msg_1 = \{CID_i, M_1, T_1\}$ →		
	Decrypt CID_i with (p, q) to obtain $(ID_i^*, R_i^*, R_i^*, T_1)$; If T_1 is not fresh, abort; $B_i' = h(ID_i \| R_i \| K)$; $M_1^* = h(ID_i \| B_i' \| R_1 \| T_1)$; If $M_1^* \neq M_1$, abort; $SK_{GW\text{-}Sj} = h(SID_j \| K)$; Generate $R2$; $M_2 = h(ID_i^* \| R_1^* \| R_i)$; $M_3 = h(h(M_2 \| \text{``1''}) \| SK_{GW\text{-}Sj} \| R_2 \| T_2)$; $M_4 = M_2 \oplus h(SK_{GW\text{-}Sj} \| T_2)$; $M_5 = R_2 \oplus (SK_{GW\text{-}Sj} \| SID_j \| T_2)$; $msg_2 = \{M_3, M_4, M_5, T_2\}$ →	
		If T_2 is not fresh, abort; $R_2' = M_5 \oplus (SK_{GW\text{-}Sj} \| SID_j \| T_2)$; $M_2 = M_4 \oplus h(SK_{GW\text{-}Sj} \| T_2)$; If $M_3 \neq h(h(M_2 \| \text{``1''}) \| SK_{GW\text{-}Sj} \| R_2' \| T_2)$, abort; Choose R_3; $SK = h(M_2' \| R_2' \| R_3)$; $M_6 = h(SK \| R_3 \| SK_{GW\text{-}Sj})$; $M_7 = h(R_2' \| T_3) \oplus R_3$; $msg_3 = \{M_6, M_7, T_3\}$ ←
	If T_3 is not fresh, abort; $R_3' = M_7 \oplus h(R_2' \| T_3)$; $SK' = h(M_2 \| R_2 \| R_3')$; $M_6' = h(SK' \| R_3' \| SK_{GW\text{-}Sj})$; If $M_6' \neq M_6$, abort; $M_8 = R_2 \oplus h(ID_i^* \| R_i^*)$; $M_9 = R_3 \oplus h(ID_i^* \| R_i^*)$; $M_{10} = h(ID_i^* \| SK' \| R_3 \| T_4)$; $msg_4 = \{M_8, M_9, M_{10}, T_4\}$ ←	
If T_4 is not fresh, abort; $R_2' = M_8 \oplus h(ID_i \| R_1)$; $R_3' = M_9 \oplus h(ID_i \| R_2')$; $SK^* = h(h(ID_i \| R_1 \| R_i') \| R_2' \| R_3')$; If $M_{10} = h(ID_i \| SK^* \| R_3' \| T_4)$, accept SK^*.		

Figure 2: The login and authentication phase of the improved protocol.

At last, MD contains the information $\{\mathrm{Reg}_i^{\mathrm{new}}, A_i^{*\mathrm{new}}, C_i^{\mathrm{new}}, m, n, h()\}$.

5. Security Analysis and Performance Comparison

In this section, we evaluate the security of our proposal under the random oracle model [48] and a comprehensive heuristic security analysis. In addition, the performance comparisons with relevant competitive schemes are made.

5.1. Authentication Proof Based on Random Oracle Model. In this section, we use the random oracle model to provide an authentication proof of the proposal. For simplicity, we present our formal security proof based on the security model of the previous works [48, 49].

Theorem 1. *Suppose A is a polynomial time-bounded attacker running in time t_A and let $Adv^{AKE}_{P,D_{PW}}(A)$ be the advantage of A in breaking the semantic security of the improved authenticated key exchanged (AKE) scheme P and $Adv^{RAE}_{A}(t)$ be the advantage of the attacker A in cracking robust authenticated encryption (RAE) [50] in polynoamial time t. To break the semantic security of the proposed scheme, A asks at most q_s times Send queries, q_e times Execute queries, and q_h times Hash queries. Thus, we have*

$$Adv^{AKE}_{P,D_{PW}}(A) \le \frac{4q_s + q_h^2}{2^{l_s}} + \frac{(q_s+q_e)^3}{2^{l_r+1}} + \frac{2q_s}{|D_{PW}|} + 2q_h\left(1+(q_s+q_e)^2\right)Adv^{RAE}_{A}(t_A), \tag{1}$$

where l_s denotes the security parameter, l_r denotes the length of the random number, D_{PW} denotes a password dictionary with a frequency distribution following Zipf's law [51], and $|D_{PW}|$ denotes the size of D_{PW}.

Proof. A set of hybrid games Gm_i ($i = 0, 1, 2, 3, 4, 5$) are completed in the proof. S_i represents the event that the attacker successfully guesses a correct bit in the *Test* query in each G m_i, and $Pr[S_i]$ represents the probability of S_i. The details of each game are described as follows.

Gm_0: this starting game is considered identical to a real attack scenario under random oracle model. Thus, we have

$$\mathrm{Adv}^{\mathrm{AKE}}_{P,D_{\mathrm{PW}}}(A) = 2\ \mathrm{Pr}\ [S_0] - 1. \tag{2}$$

Gm_1: according to the improved scheme, this game simulates queries including *Test*, *Execute*, *Send*, *Hash*, and *Corrupt*. And three lists L_h, L_A, and L_T are created to store the answer of various oracles. We can see that the simulation of Gm_1 is indistinguishable to execution of Gm_0. Thus, we have

$$\mathrm{Pr}\ [S_1] = \mathrm{Pr}\ [S_0]. \tag{3}$$

Gm_2: in this game, we consider the collisions of random oracle query and random numbers in protocol *P*. If the collision of hash oracle and transcripts msg_1, msg_2, msg_3, and msg_4 occurs, the simulator aborts and lets the attacker win the game. According to the birthday paradox, the collision probability of the hash oracle is $q_h^2/2^{l_s+1}$ at most, and the collision probability of random numbers R_1, R_2, and R_3 is $(\mathrm{q_s} + \mathrm{q_e})^3/2^{\mathrm{l_r}+2}$. Thus, we have

$$|\mathrm{Pr}\ [S_2] - \mathrm{Pr}\ [S_1]| \le \frac{q_h^2}{2^{l_s+1}} + \frac{(q_s+q_e)^3}{2^{l_r+2}}. \tag{4}$$

Gm_3: in this game, all the oracles are simulated as the previous game. If the attacker guesses M_1, M_3, M_6, and M_{10} without making corresponding $h()$ queries, the simulation will terminate. Thus, Gm_3 and Gm_2 are indistinguishable, and we have

$$|\mathrm{Pr}\ [S_3] - \mathrm{Pr}\ [S_2]| \le \frac{q_s}{2^{l_s}}. \tag{5}$$

Gm_4: in this game, we take into account both online and offline attacks performed by the attacker. This game can be demonstrated as two cases. The first denotes online guessing attack, and the second denotes offline guessing attack.

Case 1. The attacker asks $Corrupt(U_i^{\mu}, 1)$ to guess PW_i and r_i. So, two subcases are considered as follows:

Case 1.1. The attacker chooses a password from D_{PW} online and simulates $Send(U_i^{\mu}, \mathrm{GWN}^{\lambda}, \mathrm{msg}_1)$ query q_s times. Thus, the collision probability is $\mathrm{q_s}/|D_{\mathrm{PW}}|$.

Case 1.2. We consider the situation that the attacker guesses r_i online intentionally or accidentally, and the collision probability is $\mathrm{q_s}/2^{\mathrm{l_s}}$ at most.

Case 2. To launch offline guessing attack, the attacker asks $Corrupt(U_i^{\mu}, 1)$ along with $Corrupt(U_i^{\mu}, 0)$ query, as well as *Execute* and *Send* queries. Then, *Hash* oracle will be queried at least q_h times, and the simulation will be terminated once an invalid value is returned. Thus, the collision probability is at most $q_h\mathrm{Adv}^{\mathrm{RAE}}_{A}(t_A)$.

According to the analysis of the above cases, we have

$$|\mathrm{Pr}\ [S_4] - \mathrm{Pr}\ [S_3]| \le \frac{q_s}{|D_{\mathrm{PW}}|} + \frac{q_s}{2^{l_s}} + q_h\mathrm{Adv}^{\mathrm{RAE}}_{A}(t_A). \tag{6}$$

Gm_5: in this game, the attacker executes *Send*, *Execute*, and *Hash* oracle queries on transcripts to break strong forward security. After choosing two indices from $\{1, 2, \cdots, q_s + q_e\}$, the attacker executes a *Test* oracle and asks $Corrupt(U_i^{\mu} \setminus \mathrm{GWN}^{\lambda} \setminus S_j^{\nu})$. The simulation will abort if the *Test* oracle cannot return the session key for the *i*th instance of U_i and the *j*th instance of S_j. Thus, we have

$$|\mathrm{Pr}\ [S_5] - \mathrm{Pr}\ [S_4]| \le q_h(q_s+q_e)^2\mathrm{Adv}^{\mathrm{RAE}}_{A}(t_A). \tag{7}$$

Considering all the games, the attacker has no advantage in surmising the correct bit *b*. Thus, we have

$$\Pr[S_5] = \frac{1}{2}. \quad (8)$$

Using equations (2)–(8), the theorem is proved.

5.2. Analysis of Security Features. This section provides an informal security analysis, which demonstrates that the proposed scheme not only overcomes the security weaknesses in Jiang et al.'s scheme but also withstands various attacks.

(1) *Resistance to Stolen Mobile Device Attack*. Assume that MD is acquired by the attacker, and he extracts the secret data $\{\text{Reg}_i, A_i, C_i, D_i, m, n, h()\}$ by power analysis [42] or side-channel technique [43]. From the medical professional registration phase, we can see that $\text{Reg}_i = h(h(\text{ID}_i \| R_i \| \text{HPW}_i) \bmod m)$, where $\text{HPW}_i = h(r_i \oplus \text{PW}_i)$. If the attacker tries to guess the ID_i and PW_i via $\text{Reg}_i = h(h(\text{ID}_i \| R_i \| h(r_i \oplus \text{PW}_i)) \bmod m)$, he will not succeed since R_i and r_i are sufficiently large and he cannot guess them in polynomial time according to item 4 of the adversary model in Section 3.1. Furthermore, the attacker can get $C_i = B_i \oplus h(\text{ID}_i \| R_i \| \text{HPW}_i)$ where $B_i = h(\text{ID}_i \| R_i \| K)$, but he will also fail when he launches an offline dictionary attack on ID_i and PW_i because R_i and K are sufficiently large. Therefore, the proposal can withstand stolen mobile device attack

(2) *Resistance to Privileged Insider Attack*. Suppose that a privileged insider has obtained the user's registration request $\{\text{ID}_i, \text{HPW}_i\}$, and he also gets the user's mobile device that contains secret information $\{\text{Reg}_i, A_i, C_i, D_i, m, n, h()\}$, where $\text{Reg}_i = h(h(\text{ID}_i \| R_i \| \text{HPW}_i) \bmod m)$, $A_i^* = A_i \oplus h(\text{ID}_i \| r_i) = R_i \oplus h(r_i \oplus \text{PW}_i)$, $C_i = B_i \oplus h(\text{ID}_i \| R_i \| \text{HPW}_i)$, $D_i = r_i \oplus h(h(\text{ID}_i \| \text{PW}_i) \bmod m)$, and $B_i = h(\text{ID}_i \| R_i \| K)$. If the attacker chooses a pair $(\text{ID}_i, \text{PW}_i)$ from $D_{\text{ID}} \times D_{\text{PW}}$ to perform offline password guessing attack via $r_i = D_i \oplus h(h(\text{ID}_i \| \text{PW}_i) \bmod m)$ and $\text{HPW}_i = h(r_i \oplus \text{PW}_i)$, and we set $|D_{\text{PW}}| = |D_{\text{ID}}| = 10^6$ and $m = 2^8$ [51, 52], it can be assured that there are $|D_{\text{ID}}| * |D_{\text{PW}}|/\text{m} \approx 2^{32}$ candidates $(\text{ID}_i, \text{PW}_i)$ to prevent the attacker from guessing out the correct password. Moreover, if the insider attacker tries to compromise PW_i from A_i^* or C_i, he will still fail since he does not know random numbers r_i and R_i and the long-term key K. Therefore, the proposal can resist privileged insider attack

(3) *Resistance to KSSTI Attack*. In our scheme, the session key $\text{SK} = h(M_2 \| R_2 \| R_3) = h(h(\text{ID}_i \| R_1 \| R_i) \| R_2 \| R_3)$ is generated with the parameters ID_i, R_i, R_1, R_2, and R_3, which are provided by the mobile device, GWN, and sensor, respectively. If the attacker captures messages $\text{msg}_2 = \{M_3, M_4, M_5, T_2\}$ and $\text{msg}_3 = \{M_6, M_7, T_3\}$, we discuss that the proposed scheme can resist *KSSTI* attack in three cases.

Case 1. Suppose R_2 is compromised. It is clear that the attacker can calculate $R_3 = M_7 \oplus h(R_2 \| T_3)$. To obtain M_2, the attacker intends to compute $M_2 = M_4 \oplus h(\text{SK}_{\text{GW}-Sj} \| T_2)$. However, the attacker knows nothing about $\text{SK}_{\text{GW}-Sj}$, SID_j, and K, resulting in failure of computing M_2 by $M_2 = M_4 \oplus h(\text{SK}_{\text{GW}-Sj} \| T_2)$. Thus, the attacker cannot compute the session key if R_2 is compromised.

Case 2. Suppose R_3 is compromised. To get R_2, the attacker first computes $h(R_2 \| T_3) = M_7 \oplus \text{R}_3$, and $h(\text{ID}_i \| R_2) = M_9 \oplus R_3$ and then mounts an offline guessing attack. However, he will be unsuccessful according to item 4 of the adversary model in Section 3.1. Moreover, he cannot compute M_2 by $M_2 = M_4 \oplus h(\text{SK}_{\text{GW}-Sj} \| T_2)$ as we analyzed in Case 1. Thus, his dream will not come true in computing the session key $\text{SK} = \text{h}(M_2 \| R_2 \| R_3)$.

Case 3. Suppose R_1 is compromised. In our protocol, if the attacker attempts to derive R_2 by computing $R_2 = \text{M}_8 \oplus h(\text{ID}_i \| R_1)$, the attacker has to know the identity ID_i of the user. However, it is impossible for him to retrieve ID_i from other components in the public messages. Thus, the attacker cannot calculate the session key if he only knows R_1.

(4) *Resistance to GWN Impersonation Attack*. During the authentication protocol execution, if the attacker makes an effort to masquerade GWN, he has to generate messages $\{M_3, M_4, M_5, T_2\}$ and $\{M_8, M_9, M_{10}, T_4\}$ and transmit them to S_j and U_i, respectively, where $M_3 = h(h(M_2 \| \text{“}1\text{”}) \| \text{SK}_{\text{GW}-Sj} \| R_2 \| T_2)$, $M_4 = M_2 \oplus h(\text{SK}_{\text{GW}-Sj} \| T_2)$, $M_5 = R_2 \oplus (\text{SK}_{\text{GW}-Sj} \| \text{SID}_j \| T_2)$, $M_2 = h(\text{ID}_i^* \| R_1^* \| R_i)$, $M_8 = R_2 \oplus h(\text{ID}_i^* \| R_1^*)$, $M_9 = R_3 \oplus h(\text{ID}_i \| R_2)$, and $M_{10} = h(\text{ID}_i^* \| \text{SK}' \| R_3 \| T_4)$. However, without the knowledge of $(\text{SID}_j, K, \text{ID}_i)$ and $(R_1, R_2, R_3, \text{SK})$, the attacker is unable to generate these two messages to cheat the sensor and the user. Hence, the proposal can withstand GWN impersonation attack

(5) *Resistance to Desynchronization Attack*. There are two conditions that may lead to desynchronization attack. First, both parties of communication stored authentication data that needs to be updated simultaneous, and if the message sent from one party to the other is intercepted by the attacker, the result is that the authentication data in one party has been updated whereas the other party's is still unchanged. In our protocol, MD and the sensor are not required to update their authentication data simultaneously. Second, the authenticated protocol needs to maintain verification tables in GWN, or the server is subject to this attack. However, our improved scheme is not required to store a verification table in GWN. In short, our improved scheme is free from desynchronization attack

(6) *Resistance to Sensor Impersonation Attack*. In this attack, the attacker generates a valid message $\{M_6, M_7, T_3\}$ to cheat the GWN. However, because S K_{GW-Sj} is carefully protected by the GWN and the attacker has no knowledge of R_2 and R_3, the attacker cannot succeed in forging the message $\{M_6, M_7, T_3\}$. Therefore, the improved scheme is able to resist sensor impersonation attack

(7) *Resistance to Replay Attack and Man-in-the-Middle Attack*. Generally, random nonce and timestamp are the two main techniques to prevent replay attack in authentication protocol. In our improved scheme, if the attacker captures the login message $\{CID_i, M_1, T_1\}$ and replays it to GWN, he cannot be authenticated by GWN because GWN will check the freshness of T_1 and verify the hash value M_1 which is computed with secret random numbers R_i and R_1 shared between mobile device and the sensor. In addition, if the attacker generates an imitated login message with a new timestamp $T_1{}'$, the GWN will reject it because $T_1{}'$ should be a parameter of M_1, and M_1 cannot pass the verification of GWN. Thus, the improved scheme is secured from replay attack. Moreover, without knowing $(ID_i, R_i, R_1, R_2, R_3)$, the attacker is unable to compute the session key $SK = h(M_2\|R_2\|R_3)$. Hence, the attacker will fail in passing the authentication of the sensor S_j, which means he cannot produce a valid session with S_j via retransmitting the request message of U_i. Thus, the proposal can thwart man-in-the-middle attack

(8) *Perfect Forward and Backward Secrecy*. As can be seen from the login and authentication phase, the session key $SK = h(M_2\|R_2\|R_3) = h(h(ID_i\|R_1\|R_i)\|R_2\|R_3)$ is computed by U_i and S_j, and it relies on $(ID_i, R_i, R_1, R_2, R_3)$, where the parameters (R_i, R_1, R_2, R_3) are randomly generated and unpredictable. Even if the attacker knows the leaked long-term key K of GWN, it is still impossible for him to calculate the session key because he has no knowledge of these random numbers provided by each communication party, i.e., U_i, GWN, and S_j. That is to say, the improved protocol can provide perfect forward and backward secrecy

(9) *Resistance to User Impersonation Attack*. Assume that the attacker obtains the mobile device and extracts the secret information $\{Reg_i, A_i{}^*, C_i, D_i, m, n, h()\}$, where $Reg_i = h(h(ID_i\|R_i\|HPW_i) \bmod m)$, $A_i{}^* = A_i \oplus h(ID_i\|r_i)$, $C_i = B_i \oplus h(ID_i\|R_i\|HPW_i)$, $D_i = r_i \oplus h(h(ID_i\|PW_i) \bmod m)$, and $B_i = h(ID_i\|R_i\|K)$. To generate a valid login request $\{CID_i, M_1, T_1\}$, the attacker should first derive both password and mobile device of the medical professional. In particular, GWN validates the legitimacy of the medical professional by checking $M_1 ? = h(ID_i\|B_i\|R_1\|T_1)$, and the key to compute M_1 is to get the value of B_i. However, without the knowledge of parameters (ID_i, PW_i, R_i, and K), the attacker cannot compute B_i, which means the attacker's legitimacy will not be corroborated by GWN. Hence, the improved scheme is secure from user impersonation attack

(10) *User Anonymity*. User anonymity is extremely important in preserving the patient's privacy. Suppose that the attacker intercepts all the messages of the parties involved during the protocol execution, and in these messages, the component CI $D_i = (ID_i\|R_1\|R_i{}^*\|SID_j)^2 \bmod n$ is related to the identity of the medical professional directly. However, the attacker cannot decrypt CID_i to get ID_i because he has no knowledge of n or (p, q). Besides, if the attacker attempts to mount identity guessing attack on M_8, M_9, and M_{10}, respectively, where

Table 2: Comparison of security features.

	[27]	[29]	[33]	[53]	[54]	Ours
S1	Yes	Yes	No	No	Yes	Yes
S2	No	No	No	No	Yes	Yes
S3	Yes	Yes	Yes	Yes	Yes	Yes
S4	Yes	Yes	Yes	Yes	Yes	Yes
S5	Yes	Yes	Yes	Yes	Yes	Yes
S6	Yes	No	No	Yes	Yes	Yes
S7	Yes	Yes	Yes	Yes	Yes	Yes
S8	Yes	No	No	Yes	No	Yes
S9	Yes	No	Yes	No	No	Yes
S10	Yes	Yes	Yes	Yes	Yes	Yes
S11	No	Yes	No	No	Yes	Yes
S12	Yes	No	No	Yes	Yes	Yes
S13	Yes	Yes	Yes	Yes	Yes	Yes

S1: resisting stolen mobile device attack; S2: resisting user impersonation attack; S3: resisting GWN impersonation attack; S4: resisting sensor node impersonation attack; S5: resisting desynchronization attack; S6: resisting KSSTI attack; S7: perfect forward and backward secrecy; S8: resisting replay attack; S9: resisting privileged insider attack; S10: resisting man-in-the-middle attack; S11: user anonymity; S12: sensor anonymity; S13: mutual authentication and key agreement.

Table 3: Execution time of cryptographic operation.

Notation	Meaning	Time (ms)
T_h	Time of a hash operation	0.0004 [53]
T_m	Time of a modular squaring	$=T_h$ [41]
T_P	Time of ECC point multiplication	7.3529 [44]
T_s	Time of symmetric encryption/decryption	0.1303 [44]
T_{QR}	Time of square root modular n	1.8382 [41, 44]
T_R	Time of Rep operation	$=T_P$ [53]

Table 4: Performance comparison.

	[27]	[29]	[33]	[53]	[54]	Ours
U_i	$8T_h + T_R + 2T_S$	$9T_h + T_M$	$11T_h + T_R + 2T_P$	$9T_h + T_R + 2T_S$	$10T_h + 3T_P$	$11T_h + T_M$
GWN	$7T_h + 6T_S$	$14T_h + T_{QR}$	$10T_h$	$13T_h + 2T_S$	$8T_h + T_P$	$13T_h + T_{QR}$
S_j	$5T_h + 2T_S$	$7T_h$	$3T_h + 2T_P$	$5T_h$	$4T_h + 2T_P$	$7T_h$
Total cost	$20T_h + T_R + 10T_S$	$30T_h + 6T_M + T_{QR}$	$24T_h + T_R + 4T_P$	$27T_h + T_M + 4T_S$	$22T_h + 6T_P$	$31T_h + 6T_M + T_{QR}$
Estimated time (ms)	8.66	1.84	36.77	7.88	51.61	1.97
Communication overhead (bits)	2944	2560	3072	2496	2880	2592

$M_8 = R_2 \oplus h(\mathrm{ID}_i^* \| R_1^*)$, $M_9 = R_3 \oplus h(\mathrm{ID}_i^* \| R_2^*)$, and $M_{10} = h(\mathrm{ID}_i^* \| \mathrm{SK}' \| R_3 \| T_4)$, he will not succeed because the random numbers R_1, R_2, and R_3 are adequately large to prevent him from guessing them out successfully. Therefore, the improved scheme is capable of preserving user anonymity

(11) *Mutual Authentication and Key Agreement*. Due to the insecure nature of the wireless channel, mutual authentication has become one of the essential security features in authentication protocol. In the login and authentication phase, GWN authenticates U_i, S_j authenticates GWN, GWN authenticates S_j, and U_i authenticates GWN. Meanwhile, the shared session key $\mathrm{SK} = h(h(\mathrm{ID}_i \| R_1 \| R_i) \| R_2 \| R_3)$ is generated between U_i and S_j for future secure communication after authenticating each other successfully

5.3. Security and Performance Comparison. In this section, we compare the security features and performances of the improved scheme with the relevant competitive schemes [27, 29, 33, 53, 54].

Table 2 shows the comparison results of security features between the improved scheme and the related ones [27, 29, 33, 53, 54]. From Table 2, it is evident that our scheme has overcome the security weaknesses existing in Jiang et al.'s scheme [29], while the other protocols have security vulnerabilities more or less, e.g., protocols [27, 29, 33] suffer from user impersonation attack and cannot preserve user anonymity, protocols [53, 54] are vulnerable to stolen mobile device attack, and protocol [54] cannot resist replay and privileged insider attack. Particularly, some protocols [33, 53] cannot resist user impersonation attack when the mobile device is obtained by the attacker.

To facilitate the comparison of performances during the login and authentication phase, we use the various time notations of cryptographic operation as shown in Table 3. To make a comparison of computation cost fairly, we also provide the time cost of various cryptographic calculations as the benchmark [41, 44, 53] in Table 3. Additionally, we assume that the length of an identity, a random number, a hash value, a timestamp, an elliptic curve point, the block size of AES symmetric encryption/decryption, and the modular exponentiation are 32 bits, 128 bits, 160 bits, 32 bits, 320 bits, 128 bits [55], and 1024 bits [14], respectively. The comprehensive study of the improved scheme and the related schemes [27, 29, 33, 53, 54] is given in Table 4. Furthermore, the performances of the sensor node are summarized in Table 5, because energy consumption is vital to evaluate the lifetime of the sensor node. For the convenience of understanding, the comparison graphs of computation cost, communication overhead, and traffic of sensor node are shown in Figures 3, 4, and 5, respectively.

In Table 4, it is evident that the protocol [29] is the most efficient one in terms of computation cost and communication overhead. Our improved scheme requires a little more computation cost and communication overhead than protocol [29]. However, the performance of our improved scheme is more efficient than protocols [27, 33, 53, 54] as justified from Table 4. In particular, protocols [33, 54] are the two most inefficient schemes among all the schemes since they employ ECC in which point multiplication needs more time than other operations, and elliptic curve point also needs more length than other symbols in communication.

From Table 5, it can be seen that the traffic length of sensor node in our protocol is 864 bits, which is just slightly higher than that in [29], but much lower than those in [27, 33, 53, 54]. Therefore, the potential energy consumption of our improved scheme is keeping at a manageable level for WMHS that helps to prolong the lifetime of the sensor.

Although our scheme is not the most efficient one, it is worth noting that the security analysis and the comparison results of security features in Table 2 have shown that our improved scheme overcomes the security risks in [27, 29, 33, 53, 54]. In a word, our improved scheme has higher security level while its computation cost and communication overhead are within reasonable level for WMHS environment.

6. Conclusion

To defeat the subtle security weaknesses like KSSTI attack, privileged insider attack, and DoS attack in Jiang et al.'s protocol for WMHS, we propose an improved two-factor authenticated key agreement protocol using quadratic residues. The completeness and validity of the improved scheme is proved under the random oracle model. Additionally, we provide a security analysis to demonstrate that the improved scheme is secure against various known attacks.

Table 5: Traffic comparison of sensor node.

	[27]	[29]	[33]	[53]	[54]	Ours
Receive	544	512	640	864	640	512
Send	672	320	640	352	640	352
Total	1216	832	1280	1216	1280	864

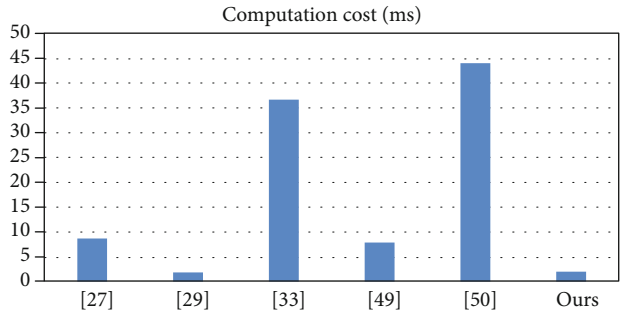

Figure 3: Comparison of computation cost.

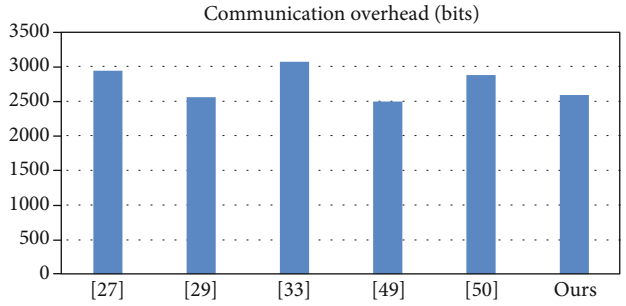

Figure 4: Comparison of communication overhead.

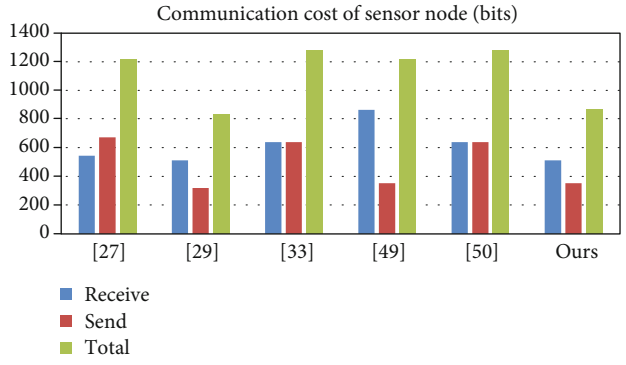

Figure 5: Comparison on traffic of sensor node.

Furthermore, performance comparisons between the improved scheme and the related ones demonstrate that our scheme outperforms the previous ones with regard to security features, computation cost, and communication overhead. Owing to these metrics, we believe that our improved scheme provides a reasonable solution for practical use in WHMS environment.

Data Availability

1. The [27] data used to support the findings of this study have been deposited in the [Springer] repository ([DOI: 10.1007/s11277-016-3718-6]). 2. The [29] data used to support the findings of this study have been deposited in the [Elsevier] repository ([DOI: 10.1016/j.compeleceng.2017.03.016]). 3. The [33] data used to support the findings of this study have been deposited in the [Springer] repository ([DOI: 10.1007/s12652-018-1015-9]). 4. The [53] data used to support the findings of this study have been deposited in the [Springer] repository ([DOI: 10.1007/s12083-016-0485-9]). 5. The [54] data used to support the findings of this study have been deposited in the [IEEE Xplore] repository ([DOI: 10.1109/JSYST.2019.2899580]).

Conflicts of Interest

The authors declare no conflict of interest regarding the publication of this paper.

Acknowledgments

This work was partially supported by the National Natural Science Foundation of China (Project No. 61672007) and Science and Technology Innovation Guidance Project 2017 (Project No. 201704030605).

References

[1] R. Amin and G. P. Biswas, "A secure three-factor user authentication and key agreement protocol for TMIS with user anonymity," *Journal of Medical Systems*, vol. 39, no. 8, 2015.

[2] S. A. Chaudhry, H. Naqvi, and M. K. Khan, "An enhanced lightweight anonymous biometric based authentication scheme for TMIS," *Multimedia Tools and Applications*, vol. 77, no. 5, pp. 5503–5524, 2018.

[3] F. Wei, P. Vijayakumar, J. Shen, R. Zhang, and L. Li, "A provably secure password-based anonymous authentication scheme for wireless body area networks," *Computers & Electrical Engineering*, vol. 65, pp. 322–331, 2018.

[4] 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, 2018.

[5] L. Zhang, Y. Zhang, S. Tang, and H. Luo, "Privacy protection for e-health systems by means of dynamic authentication and three-factor key agreement," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 3, pp. 2795–2805, 2018.

[6] O. Mir and M. Nikooghadam, "A secure biometrics based authentication with key agreement scheme in telemedicine networks for e-health services," *Wireless Personal Communications*, vol. 83, no. 4, pp. 2439–2461, 2015.

[7] Q. Jiang, M. K. Khan, X. Lu, J. Ma, and D. He, "A privacy preserving three-factor authentication protocol for e-health clouds," *The Journal of Supercomputing*, vol. 72, no. 10, pp. 3826–3849, 2016.

[8] Y. K. Ever, "Secure-anonymous user authentication scheme for e-healthcare application using wireless medical sensor networks," *IEEE Systems Journal*, vol. 13, no. 1, pp. 456–467, 2019.

[9] M. M. Baig, H. Gholamhosseini, and M. J. Connolly, "A comprehensive survey of wearable and wireless ECG monitoring systems for older adults," *Medical & Biological Engineering & Computing*, vol. 51, no. 5, pp. 485–495, 2013.

[10] Z. Yang, Q. Zhou, L. Lei, K. Zheng, and W. Xiang, "An IoT-cloud based wearable ECG monitoring system for smart healthcare," *Journal of Medical Systems*, vol. 40, no. 12, 2016.

[11] Y. Yin, H. Jiang, S. Feng et al., "Bowel sound recognition using SVM classification in a wearable health monitoring system," *Science China Information Sciences*, vol. 61, no. 8, 2018.

[12] V. Trovato, C. Colleoni, A. Castellano, and M. R. Plutino, "The key role of 3-glycidoxypropyltrimethoxysilane sol–gel precursor in the development of wearable sensors for health monitoring," *Journal of Sol-Gel Science and Technology*, vol. 87, no. 1, pp. 27–40, 2018.

[13] X. Li, F. Wu, M. K. Khan, L. Xu, J. Shen, and M. Jo, "A secure chaotic map-based remote authentication scheme for telecare medicine information systems," *Future Generation Computer Systems*, vol. 84, pp. 149–159, 2018.

[14] P. Chandrakar and H. Om, "An efficient two-factor remote user authentication and session key agreement scheme using Rabin cryptosystem," *Arabian Journal for Science and Engineering*, vol. 43, no. 2, pp. 661–673, 2018.

[15] J. Srinivas, D. Mishra, S. Mukhopadhyay, and S. Kumari, "Provably secure biometric based authentication and key agreement protocol for wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 4, pp. 875–895, 2018.

[16] M. Wazid, A. K. Das, S. Kumari, X. Li, and F. Wu, "Design of an efficient and provably secure anonymity preserving three-factor user authentication and key agreement scheme for TMIS," *Security and Communication Networks*, vol. 9, no. 13, pp. 1983–2001, 2016.

[17] F. Wu, L. Xu, S. Kumari, and X. Li, "A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client–server networks," *Computers & Electrical Engineering*, vol. 45, pp. 274–285, 2015.

[18] K.-J. Hu, H. L. Yeh, W. K. Shih, and T. H. Chen, "Robust elliptic curve cryptography-based three factor user authentication providing privacy of biometric data," *IET Information Security*, vol. 7, no. 3, pp. 247–252, 2013.

[19] R. Amin, S. H. Islam, G. P. Biswas, M. K. 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, 2016.

[20] 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, 2015.

[21] 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, 2015.

[22] C. T. Li, C. C. Lee, and C. Y. Weng, "A secure cloud-assisted wireless body area network in mobile emergency medical care system," *Journal of Medical Systems*, vol. 40, no. 5, 2016.

[23] C. H. Liu and Y. F. Chung, "Secure user authentication scheme for wireless healthcare sensor networks," *Computers & Electrical Engineering*, vol. 59, pp. 250–261, 2017.

[24] 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.

[25] 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.

[26] M. K. Khan and S. Kumari, "An improved user authentication protocol for healthcare services via wireless medical sensor networks," *International Journal of Distributed Sensor Networks*, vol. 10, no. 4, Article ID 347169, 2014.

[27] 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.

[28] 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.

[29] 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 & Electrical Engineering*, vol. 63, pp. 182–195, 2017.

[30] K. H. Rosen, *Elementary Number Theory and Its Applications*, Addison-Wesley, Reading, MA, USA, 1988.

[31] C.-G. Ma, D. Wang, and S. D. Zhao, "Security flaws in two improved remote user authentication schemes using smart cards," *International Journal of Communication Systems*, vol. 27, no. 10, pp. 2215–2227, 2015.

[32] 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 & Electrical Engineering*, vol. 69, pp. 534–554, 2018.

[33] 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*, 2018.

[34] 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, pp. 956–963, 2016.

[35] 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.

[36] 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, pp. 117–123, 2018.

[37] D. Wang and P. Wang, "Two birds with one stone: two-factor authentication with security beyond conventional bound," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 1–722, 2016.

[38] H. Krawczyk, "HMQV: a high-performance secure Diffie-Hellman protocol," in *Advances in Cryptology – CRYPTO 2005. CRYPTO 2005*, V. Shoup, Ed., vol. 3621 of Lecture Notes in Computer Science, pp. 546–566, Springer, Berlin, Heidelberg, 2005.

[39] S. Kumari, M. K. Khan, and M. Atiquzzaman, "User authentication schemes for wireless sensor networks: a review," *Ad Hoc Networks*, vol. 27, pp. 159–194, 2015.

[40] C. Wang, G. Xu, and J. Sun, "An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks," *Sensors*, vol. 17, no. 12, p. 2946, 2017.

[41] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, L. Leng, and N. Kumar, "Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks," *Computer Networks*, vol. 101, pp. 42–62, 2016.

[42] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, Springer Science & Business Media, 2010.

[43] T. H. Kim, C. K. Kim, and I. H. Park, "Side channel analysis attacks using AM demodulation on commercial smart cards with SEED," *Journal of Systems and Software*, vol. 85, no. 12, pp. 2899–2908, 2012.

[44] Q. Jiang, S. Zeadally, J. Ma, and D. He, "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks," *IEEE Access*, vol. 5, pp. 3376–3392, 2017.

[45] Y. Choi, Y. Lee, J. Moon, and D. Won, "Security enhanced multi-factor biometric authentication scheme using bio-hash function," *PLoS One*, vol. 12, no. 5, article e0176250, 2017.

[46] W. Li, Y. Shen, and P. Wang, "Breaking Three Remote User Authentication Systems for Mobile Devices," *Journal of Signal Processing Systems*, vol. 90, no. 8-9, pp. 1179–1190, 2018.

[47] A. K. Das, "A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks," *Peer-to-Peer Networking and Applications*, vol. 9, no. 1, pp. 223–244, 2016.

[48] M. Bellare and P. Rogaway, "Random oracles are practical: a paradigm for designing efficient protocols," in *Proceedings of the 1st ACM conference on Computer and communications security - CCS '93*, pp. 62–73, Fairfox, VA, USA, 1993.

[49] J. Mo and H. Chen, "A lightweight secure user authentication and key agreement protocol for wireless sensor networks," *Security and Communication Networks*, vol. 2019, Article ID 2136506, 17 pages, 2019.

[50] V. T. Hoang, T. Krovetz, and P. Rogaway, "Robust authenticated-encryption AEZ and the problem that it solves," in *Advances in Cryptology – EUROCRYPT 2015. EUROCRYPT 2015*, E. Oswald and M. Fischlin, Eds., vol. 9056 of Lecture Notes in Computer Science, pp. 15–44, Springer, Berlin, Heidelberg, 2015.

[51] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's law in passwords," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2776–2791, 2017.

[52] D. Wang, Z. Zhang, P. Wang, J. Yan, and X. Huang, "Targeted online password guessing: an underestimated threat," in *Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS'16)*, pp. 1242–1254, Vienna, Austria, October 2016.

[53] F. Wu, L. Xu, S. Kumari, and X. Li, "An improved and provably secure three-factor user authentication scheme for wireless sensor networks," *Peer-to-Peer Networking and Applications*, vol. 11, no. 1, pp. 1–20, 2018.

[54] X. Li, J. Peng, M. S. Obaidat, F. Wu, M. K. Khan, and C. Chen, "A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems," *IEEE Systems Journal*, vol. 14, no. 1, pp. 39–50, 2020.

[55] J. H. Burrows, *Secure hash standard*, Department of Commerce Washington DC, 1995.