Privacy-Preserving Fast Three-Factor Authentication and Key Agreement for IoT-Based E-Health Systems

Liping Zhang, Yue Zhu, Wei Ren, *Member, IEEE*, Yixin Zhang, and Kim-Kwang Raymond Choo, *Senior Member, IEEE*

Abstract—Electronic healthcare (e-health) systems have received renewed interest, particularly in the current COVID-19 pandemic (e.g., lockdowns and changes in hospital policies due to the pandemic). However, ensuring security of both data-at-rest and data-in-transit remains challenging to achieve, particularly since data is collected and sent from less insecure devices (e.g., patients' wearable or home devices). While there have been a number of authentication schemes, such as those based on three-factor authentication, to provide authentication and privacy protection, a number of limitations associated with these schemes remain (e.g., (in)security or computationally expensive). In this study, we present a privacy-preserving three-factor authenticated key agreement scheme that is sufficiently lightweight for resource-constrained e-health systems. The proposed scheme enables both mutual authentication and session key negotiation in addition to privacy protection, with minimal computational cost. The security of the proposed scheme is demonstrated in the Real-or-Random model. Experiments using Raspberry Pi show that the proposed scheme achieves reduced computational cost (of up to 89.9% in comparison to three other related schemes).

Index Terms—Electronic healthcare system, authenticated key agreement, biometric template, privacy protection

1 Introduction

As our society is going grey, there is an increasing need for more efficient healthcare services, such as those that offer remote monitoring (e.g., collecting of patient-related data, such as heartbeat and other vital signs, using wearable or home devices). According to studies, such as [1], most chronic and fatal diseases can be controlled or prevented through efficient real-time monitoring, prompt information feedback, and flexible remote treatments. The need for efficient remote, electronic healthcare (e-healthcare) is also reinforced in the COVID-19 pandemic, where the public with minor aliments or seeking elective surgery is discouraged from going to hospitals.

An e-health system can consist of a broad range of devices and systems, such as intelligent low-power biomedical sensor devices to provide timely biomedical signals (e.g., electrocardiogram (ECG), electroencephalogram (EEG), and photoplethysmography (PPG)) [2]. The collected biomedical signals will then be transmitted to hospitals or other health authorities via the Internet to facilitate continuous health monitoring and provide real-time feedback for patients. Compared with the traditional healthcare systems, e-health system can help to reduce healthcare costs, ease the burden of hospital (e.g., during pandemics), provide more convenient medical services (e.g., to residents living in rural or inaccessible areas). However, it is also important to ensure that data (e.g., patient healthcare information) collected and transmitted in an e-health system is secure, say from threats such as eavesdropping and message modification. There are real-world consequences of a successful attack. For example, false data injection can result in fatal misdiagnosis.

Several cryptographic solutions have been proposed to secure data-in-transit in e-health systems [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22]. Existing authentication systems generally use two factors. While public-key techniques are generally more secure than symmetric systems, the former tend to be more computationally expensive (e.g., due to the reliance on time-consuming operations such as bilinear operations). However the intelligent biomedical sensor devices adopted in the e-health systems have limited energy, so the authentication schemes designed for the e-health systems should not

- *Liping Zhang, Yue Zhu, and Yixin Zhang are with the School of Computer Science, China, University of Geosciences, Wuhan 430074, China. E-mail: {carolyn321, zhu_yue1203, ss.fc.xyz}@163.com.*
- *Wei Ren is with the School of Computer Science, China University of Geosciences, Wuhan 430074, China, and with the Yunnan Key Laboratory of Blockchain Application Technology, Kunming 650500, China, and also with the Henan Key Laboratory of Network Cryptography Technology, Zhengzhou 450001, China. E-mail: weirencs@cug.edu.cn.*
- *Kim-Kwang Raymond Choo is with the Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249-0631 USA. E-mail: raymond.choo@fulbrightmail.org.*

Manuscript received 13 Dec. 2020; revised 13 Dec. 2021; accepted 5 Feb. 2022. Date of publication 9 Feb. 2022; date of current version 10 Apr. 2023.
This work was supported in part by the Open Research Project of the Hubei Key Laboratory of Intelligent GeoInformation Processing under Grant KLIGIP-2019B09, in part by the Foundation of Yunnan Key Laboratory of Blockchain Application Technology under Grants 202105AG070005 and YNB202103, in part by the National Natural Science Foundation of China under Grants 62172303 and 61972366, in part by the Provincial Key Research and Development Program of Hubei under Grant 2020BAB105, and in part by the Foundation of Henan Key Laboratory of Network Cryptography Technology under Grant LNCT2020-A01. The work of Kim-Kwang Raymond Choo was supported only by the Cloud Technology Endowed Professorship.
(Corresponding author: Wei Ren.)
Digital Object Identifier no. 10.1109/TSC.2022.3149940

1939-1374 © 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.
Authorized licensed use limited to: China University of Geosciences Wuhan Campus. Downloaded on September 06,2023 at 06:15:52 UTC from IEEE Xplore. Restrictions apply.

involve the time-consuming operations, such as the scalar multiplication operations of an elliptic curve, and the bilinear operations which are widely adopted in the public key techniques. To achieve more efficient authentication, several two-factor authenticated key agreement schemes without relying on public-key techniques have been proposed. However, designing secure two-factor schemes is no easy feat [6].

In the e-health environments, there are several privacy messages, such as the user identity which needs to transmit to achieve mutual authentication and key negotiation. However, once this sensitive information is leaked, the adversary may have the ability to launch some attacks successfully. To provide high security without using public key techniques, biometric was introduced as a third factor to design the three-factor authenticated key agreement schemes for e-health systems. Biometric identification has its own advantages over smart cards and passwords methods, such as not being divulged, forgotten, lost, or stolen. Since biometric means what you are, as complementary of other two factors (smart cards, passwords), it helps to achieve high security in the design of authentication schemes. However, biometric methods have their own challenge. Given that it is not possible to replace one's biometric information, it is important to ensure that such information does not leak when used in existing systems. Obviously, the biometric adopted in the authentication design should be unknown to everyone except the patient itself. It means the biometric information should be protected, no matter whether it is stored or transmitted during the authentication process.

In some schemes, the biometric template is stored in the smart card without further protection, which is vulnerable to side-channel attacks or reverse engineering. Or the biometric template is transmitted on an insecure channel without any protection. Or the biometric information is protected by using hash functions. This case may lead to a legal user could not pass the verification process. Thus, realizing biometric protection in identification and authentication is still challenging in practice. Furthermore, Furthermore, this is clearly not realistic as there is no foolproof security system. Compounding the challenge is the need to consider inexpensive Internet of Things (IoT) devices with limited energy and computational capabilities. In other words, the authentication schemes designed for e-health systems should avoid using time-consuming operations to meet the low-energy requirement. Therefore, how to design a fast authentication scheme with privacy protection for e-health systems remains a challenging work.

In this paper, we present a fast authentication scheme with key negotiation for e-health systems. Our scheme employs three-factor authentication (i.e., smart card, password, and biometrics), and is designed to achieve user anonymity and biometric protection by encrypting the patients' identity through the session process, and secure biometrics information during the transmission. In our scheme, high entropy random integers are adopted to protect biometric templates stored in smartcards. During the transmission process, secure hash function, patients' private information, and the symmetric encryption algorithm are used to achieve the secure transmission of biometric. The correctness of the biometric can be checked by the trusted server and the smart cards using the encrypted biometric values. In the event that the information stored in the smart card is comprised, or the adversary obtains the trusted server's master key, the adversary is still unable to obtain the patients' biometrics information. In addition, the patient's real identity is protected by the asymmetric encryption algorithm during the authentication process. Further, in our schems, since each authentication message changes in every session, the attacker cannot distinguish whether two sessions come from the same patient. Therefore, our authentication method effectively protects the patient's privacy by ensuring user anonymity, user untraceability, and biometric protection. Moreover, our scheme is also designed to incur minimal computational overhead, required for deployment in an e-health system comprising resource-constrained IoT devices.

The rest of this paper is organized as follows. In Section 2, the related work is described in detail. In Section 4, we will present our proposed scheme. Then, we adopt the Real-or-Random oracle model to prove the security of our proposed scheme in Sections 5. And we evaluate the scheme's performance using Raspberry Pi in Section 6. Finally, this paper is concluded in the last section.

2 Related Work

Password-based authentication mechanisms are widely researched and some of them are applied for e-health environments [13], [14], [15], [16]. In order to achieve high security, several public-key cryptographic algorithms, such as RSA cryptosystem, Elliptic Curve Cryptography (ECC), chaotic maps, are adopted in the authenticated key agreement scheme. To protect the patient's privacy information, Hou *et al.* [9] employed RSA cryptosystem to achieve mutual authentication for healthcare systems in IoT. But, their scheme fails to provide the user anonymity feature and involves high computational costs. In order to preserve user privacy with low computational costs, dynamic identity, and chaotic maps were employed by Li *et al.* [10] to achieve authentication and key agreement for e-health systems. Unfortunately, their scheme is vulnerable to off-line password guessing attacks and cannot satisfy perfect forward secrecy. Afterwards, to enhance efficiency, Ravanbakhsh *et al.* [11] presented a security mechanism for healthcare systems using ECC. Nevertheless, their scheme cannot resist known session-specific temporary information attacks and fails to provide the perfect forward secrecy. To overcome the weaknesses, Sahoo *et al.* [12] presented a three-factor authentication scheme based on ECC for healthcare systems using IoT devices. However, the user untraceability is not satisfied in their scheme. The public-key cryptography-based schemes mentioned above have some security weaknesses and involve time-consuming operations. Therefore, these authentication schemes are not eligible for e-health environments.

To meet the requirements of low energy consumption, several light-weight authentication schemes using two factors [13], [14], [15], [16] have been suggested. In these authentication schemes, only hash functions or symmetric encryption/ decryption algorithms are employed to avoid time-consuming operations, making the performance efficient. Yang *et al.* [13] employed hash functions to construct a lightweight authenticated key agreement scheme. Although Yang *et al.*'s scheme achieves low computational costs, it fails

Authorized licensed use limited to: China University of Geosciences Wuhan Campus. Downloaded on September 06,2023 at 06:15:52 UTC from IEEE Xplore. Restrictions apply.

TABLE 1
Techniques Used and Limitations of Related Schemes

	Techniques Used	Limitations
[9]	RSA Cryptosystem	Fails to provide the user anonymity and involves high computational costs
[10]	Chaotic Maps	Fails to resist off-line password guessing attacks and fails to provide perfect forward secrecy
[11]	Elliptic Curve Cryptography	Fails to resist session-specific temporary information attacks and fails to provide perfect forward secrecy
[12]		Fails to provide the user untraceability
[13]	Hash Functions & Two factors (password, smartcard)	Fails to provide the user anonymity, user untraceability, and suffers from the stolen mobile device attacks
[14]		Fails to provide perfect forward secrecy
[15]		Fails to resist off-line password guessing attacks and fails to provide perfect forward secrecy
[16]		Fails to resist off-line password guessing attacks and fails to provide session key security
[18]	Unique biometrics and temporal credential & Three factors (password, smartcard, biometric)	Fails to resist off-line password guessing attacks and de-synchronization attacks and fails to provide session key security
[20]	Rabin cryptosystem & Three factors (password, smartcard, biometric)	Fails to resist sensor node capture attacks and fails to provide session key security
[21]	Hash Functions & Paillier & Three factors (password, smartcard, biometric)	Fails to provide user anonymity

to provide user anonymity, user untraceability, and suffers from the stolen mobile device attacks. Wu *et al.* [14] proposed an efficient authentication scheme for healthcare systems using secure one-way hash functions. But their scheme fails to satisfy perfect forward secrecy. After that, Amin *et al.*'s scheme [15] employed hash functions to establish a patient monitoring system. However, their scheme cannot realize the perfect forward secrecy and is vulnerable to to off-line password guessing attacks [17].

Wang *et al.* [6] demonstrated that the two-factor techniques have various security shortcomings being overlooked. To address the inherent security flaws of the two-factor based schemes, several three-factor authenticated key agreement schemes using the biometric template, password, and smart cards [4], [7], [11], [12], [18], [19], [20], [21], have been proposed. They prove to be more reliable and secure in comparison with the traditional two-factor authentication schemes. Compared with the traditional two-factor (smart cards, passwords) authentication schemes, the three-factor authenticated schemes provide stronger authentication and satisfy more security requirements within the reasonable computational overhead. Therefore, three-factor authenticated key agreement schemes are more suitable for the high-security-required and resource-constraint e-health systems than the traditional two-factor authentication schemes. But it suffers from the privileged insider attack and cannot satisfy the user anonymity. Unique biometrics and temporal credential were employed by Das [18] to realize mutual authentication. However, Wu *et al.* [19] argued that Das's scheme [18] could not resist off-line guessing attacks and de-synchronization attacks. Furthermore, the strong forward security could not be guaranteed in Das's scheme [18]. Rabin cryptosystem and biometric template have been introduced by Jiang *et al.* [20] to design an efficient authenticated key agreement protocol. Nevertheless, their proposed scheme cannot withstand sensor node capture attacks and is unable to provide the session key security. Besides, their scheme incurs some extra overhead owing to the usage of the verification table. Most recently, Chatterjee *et al.* [21] presented an authentication protocol in wireless body sensor networks environments using hash functions. But user anonymity was not realized in their scheme [22]. Finally, the adopted techniques and the limitations of these above schemes are summarized in Table 1.

3 Security Requirements and Models

3.1 Security Requirements

In e-health systems, patients' privacy needs to be highly protected. An authentication scheme for e-health environment should satisfy the following security requirements according to the actual situation.

1) *Resistance of Various Attacks*. The authentication scheme should withstand various prevalent attacks in the e-health environment such as replay attacks, impersonation attacks, man-in-the-middle attacks, smart card theft attacks, etc.
2) *Mutual Authentication and Session Key Security*. After performing the authentication scheme, the patient and the medical server should authenticate with each other and negotiate a session key that is only known to the authorized entity.
3) *Perfect Forward Secrecy*. The regularly updated session keys ensure the privacy of transmitted messages between the patient and the medical server. Consider that for some reason the long-term keys have been exposed, in which case the authentication scheme still needs to ensure the security of the previously transmitted messages (previous session keys).
4) *Anonymity and Untraceability*. Patients' privacy is crucial in e-health environment. The authentication scheme should ensure patients' real identity unrevealed and untraceable from the transmitted messages.
5) *Biometric Protection*. Patients should not worry that their biometric information will be exposed when accessing e-health services. Therefore, the authentication scheme should provide biometric protection when identifying patients using biometric information.

3.2 Threat Model

According to the security requirements of e-health systems, an adversary $\mathcal{A}$ against the proposed scheme is probabilistic polynomial-time (PPT) who has the following abilities:

1) $\mathcal{A}$ has complete control of the communication channel, possessing various attack capabilities during the execution of the scheme, such as interception, delay, replay, modification, and deletion;
2) $\mathcal{A}$ can launch a side-channel attack to extract the secret data stored in the user's smart card (which are B_{ir}, R, C_{ut}, N_i in the proposed scheme);
3) To model the active attacks on the trusted server, its long-time private keys (which are k_1, k_2 in the proposed scheme) are provided to $\mathcal{A}$ only when analyzing some strong security attributes (e.g., perfect forward secrecy).

3.3 Formal Security Model

We adopt Abdalla *et al.*'s Real-or-Random (ROR) model [23], a more suitable case than the original model proposed

Authorized licensed use limited to: China University of Geosciences Wuhan Campus. Downloaded on September 06,2023 at 06:15:52 UTC from IEEE Xplore. Restrictions apply.

Initialization

$ID_i \xleftarrow{R} D_{id}$; $\langle ID_t, ID_m \rangle \xleftarrow{R} D$; $pw_i \xleftarrow{R} D_{pw}$; $B_i \xleftarrow{R} D_{bio}$;
$\langle k_1, k_2 \rangle \xleftarrow{R} \{0,1\}^{l_k}$; $\langle r_1, r_2 \rangle \xleftarrow{R} \{0,1\}^{l_r}$; $sid_U^i \xleftarrow{R} \mathbb{Z}$

Queries

Send$(\Pi_U^i/\Pi_{TS}/\Pi_{MS}, message[, state_{TS}])$:

* Note that there are 4 kinds of *Send* queries in total, whose procedures are very similar to each other, namely *Send*(Π_{TS}, *message*, $state_{TS}$ =WAIT_FOR_USER), *Send*(Π_{MS}, *message*), *Send*(Π_{TS}, *message*, $state_{TS}$ =WAIT_FOR_SERVER), *Send*(Π_U^i, *message*). We only show *Send*(Π_{TS}, *message*, $state_{TS}$ =WAIT_FOR_USER) in detail.

Send$(\Pi_{TS}, message, state_{TS}$ =WAIT_FOR_USER):
  $\langle A_i^*, A_i' \rangle \leftarrow \mathcal{P}(\Pi_{TS}, message, state_{TS})$
  if $\Delta(A_i^*, A_i') ==$ INVALID **then return** $\perp$
  $m \xleftarrow{R} \{0,1\}^{l_r}$; $Auth_{tm} \leftarrow \mathcal{P}(\Pi_{TS}, message, state_{TS}, m)$
  return $Auth_{tm}$

Execute$(\Pi_U^i, \Pi_{TS}, \Pi_{MS})$:
  if $\Pi_U^i \notin \mathcal{U}$ or $\Pi_{TS} \notin \mathcal{TS}$ or $\Pi_{MS} \notin \mathcal{MS}$ **then return** $\perp$
  $\langle C_{ut}, Auth_{ut}, Auth_{tm}, Auth_{mt}, Auth_{tu} \rangle \leftarrow \mathcal{P}(\Pi_U^i, \Pi_{TS}, \Pi_{MS})$
  return $\langle C_{ut}, Auth_{ut}, Auth_{tm}, Auth_{mt}, Auth_{tu} \rangle$

Corrupt(Π_U^i):
  if $\Pi_U^i \notin \mathcal{U}$ **then return** $\perp$
  $\langle B_{ir}, R, C_{ut}, N_i \rangle \leftarrow \mathcal{P}(\Pi_U^i)$; **return** $\langle B_{ir}, R, C_{ut}, N_i \rangle$

Corrupt(Π_{TS}):
  if $\Pi_{TS} \notin \mathcal{TS}$ **then return** $\perp$
  return $\langle k_1, k_2 \rangle$

Test(sid_U^i):
  if $sid_U^i ==$ INVALID **then return** $\perp$
  $c \xleftarrow{R} \{0,1\}$; $SK \leftarrow \mathcal{P}(sid_U^i)$; $rand \xleftarrow{R} \{0,1\}^{l_h}$
  if $c == 1$ **then return** SK **else return** $rand$

Hash Oracles

Hash(x):
  Search x in table $\{x_1, x_2\}$
  if found an $x_1 == x$ **then return** x_2
  else $x_r \xleftarrow{R} \{0,1\}^{l_h}$; Insert $\langle x, x_r \rangle$ into table; **return** x_r

Biohash(y):
  Search y in table $\{y_1, y_2\}$
  if found a y_1 holds $\Delta(y_1, y) ==$ VALID **then return** y_2
  else $y_r \xleftarrow{R} \{0,1\}^{l_{bh}}$; Insert $\langle y, y_r \rangle$ into table; **return** y_r

* Note that table $\{x_1, x_2\}$ and table $\{y_1, y_2\}$ are two different tables maintained by different oracles.

Fig. 1. The detailed design of the oracle system.

by Bellare *et al*. [24], to formally simulate real attacks on the authentication scheme for e-health systems. Some of the basic concepts following their work are omitted in this paper, such as *participants*, *long-lived keys*, *freshness*, etc.

In the ROR model, the security model is defined by a game between two probabilistic polynomial-time Turing machines, namely a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$. It is assumed that $\mathcal{C}$ owes a real system that has already applied our proposed scheme $\mathcal{P}$ to it. In order to evaluate $\mathcal{P}$'s security, $\mathcal{C}$ intended to invite $\mathcal{A}$ to launch a real attack on $\mathcal{P}$, but $\mathcal{C}$ worried about $\mathcal{A}$ would learn enormous useful information about the real system. So $\mathcal{C}$ developed an oracle system and designed a game to play with $\mathcal{A}$. After initialization, the oracle flips an unbiased coin c (c=$\{0, 1\}$) and the goal of $\mathcal{A}$ is to guess the value of c. To increase the chance of winning this game, $\mathcal{A}$ is provided a series of queries to ask the oracle. These queries are defined based on the adversary's abilities we presented above.

TABLE 2
Notations and Descriptions

Notation	Descriptions
ID_i	The identity of the i^th patient U_i
ID_t	The trusted server's identity
ID_m	The medical server's identity
pw_i	The *i-th* user U_i's password
k_1, k_2	The trusted server's private keys
m, n, r_1, r_2, r_3	Five high entropy random integers
B_i	The biometric template of U_i
$E_{key}(\cdot)/D_{key}(\cdot)$	Symmetric key encryption/decryption algorithm
$h(\cdot)$	A secure one-way hash function
$h_{bio}(\cdot)$	A secure one-way biohash function
$\|\|$	The concatenation operation
$\oplus$	The exclusive-or operation
SK_{tm}	The pre-shared secret information between *TS* and *MS*
Δ	A string comparison algorithm of biometrics

Let $\prod_U^i$ denote an instance i of a user participant in a set of users $\mathcal{U}$, who has an identity of $ID_i \in D_{id}$, a password $pw_i \in D_{pw}$, and a biometric information $B_i \in D_{bio}$. And let $\prod_{TS}$ and $\prod_{MS}$ denote an instance of a trusted server and a medical server, which have an identity of $ID_t \in D$ and $ID_m \in D$, respectively. The session of $\prod_U^i$, $\prod_{TS}$, and $\prod_{MS}$ is identified by a session id sid_U^i. The notation l_k, l_r, l_h and l_{bh} denote the length of *TS*'s long-term secret key, random numbers, a hash function's output, and a biohash function's output, respectively. The detailed design of the oracle is presented in Fig. 1.

4 The Proposed Scheme

In this section, we present the proposed three-factor authentication scheme for e-health systems in detail. The new scheme is composed of three phases: registration phase, login phase, authentication and key agreement phase. To clarify the proposed authentication scheme, notations and their descriptions are summarized in Table 2. Before the registration phase, we assume that the following assumptions hold: the trusted server *TS* is a trusted entity and it has a master key k_1 and a secret key k_2. Besides, the trusted server and the medical server have a pre-shared secret information $SK_{tm} = h(ID_t||ID_m||k_2)$.

4.1 Registration Phase

In the registration phase, the patient U_i performs the following process with the trusted server *TS*:

*Step R*1. The patient U_i chooses his/her password pw_i, identity ID_i, and a high entropy random integer r_1. Then, the patient U_i selects a secure one-way hash function $h(\cdot): \{0,1\}^* \longrightarrow \{0,1\}^l$, here l is a secure parameter. Next, the patient U_i scans the iris to create a biometric template B_i, and computes $HPW = h(ID_i \oplus pw_i \oplus h_{bio}(B_i))$, $B_{ir} = B_i \oplus r_1$, $P = HPW \oplus B_{ir}$ and $R = h(ID_i||h_{bio}(B_i)||pw_i) \oplus r_1$. Here, the biohash algorithms such as [25], [26], [27] can be used to compute $h_{bio}(B_i)$. Finally, the patient U_i sends $\{ID_i, HPW, h(\cdot), P\}$ to the *TS* through a secure channel.

*Step R*2. Upon receiving $\{ID_i, HPW, h(\cdot), P\}$, the *TS* selects a random integer r_2 and computes $M_1 = ID_i \oplus ID_t$ to obtain $C_{ut} = E_{k_1}(M_1||r_2||P)$. Here, the random integer r_2 does not need to be stored in *TS*'s database. Then, the *TS* adopts its long-term private key k_1 to calculate the secret

Authorized licensed use limited to: China University of Geosciences Wuhan Campus. Downloaded on September 06,2023 at 06:15:52 UTC from IEEE Xplore. Restrictions apply.

message $N_i = h(ID_i||ID_t||k_1||r_2) \oplus HPW$. Next, the *TS* issues a smart card that contains $\{C_{ut}, N_i\}$ and sends it to the patient U_i via a secure channel.

*Step R*3. Once the patient receives the smart card, he/she will write B_{ir} and R to the smart card. And then, the information $\{h_{bio}(\cdot), h(\cdot), B_{ir}, R, C_{ut}, N_i\}$ is stored in patient's smart card.

4.2 Login Phase

In this phase, the patient's password and biometric template are verified by the smart card first. After this authentication is passed, the smart card transmits the authentication message to the trusted server for the next phase.

*Step L*1. The patient U_i inserts his/her smart card into the smart card reader, inputs the ID_i and corresponding pw_i, and performs iris scan to create the biometric template B_i^*. After that, the smart card extracts $r_1^{'} = R \oplus h(ID_i||h_{bio}(B_i)||pw_i)$ from R by using the ID_i and pw_i inputted by the patient U_i. Next, the smart card computes $B_{ir}^{'}$=$B_i^* \oplus r_1$ and compares $B_{ir}^{'}$ with the secret B_{ir} stored in its memory. Here, the Hamming distance is used to compare the two biometric strings $(B_{ir}^{'}, B_{ir})$ and the XOR operation is chosen since it will not affect the matching result. If the matching difference value $\Delta(B_{ir}^{'}, B_{ir})$ is beyond the predefined threshold, the smart card stops the session.

*Step L*2. If the user passes the identity verification, the smart card computes $HPW^{'} = h(ID_i \oplus pw_i \oplus h_{bio}(B_i^*))$ to construct the secret information $P^{'} = HPW^{'} \oplus B_{ir}^{'}$. And then the smart card chooses a high entropy random integer m to compute secret information $A_i = h(ID_i||(m \oplus ID_m)) \oplus P^{'}$ and $X_1 = h(ID_i||C_{ut}||A_i) \oplus m$. Afterwards, the smart card computes the encryption key $SK_{ut} = N_i \oplus HPW^{'}$. And it generates an authentication message $Auth_{ut} = E_{SK_{ut}}(X_1||ID_m||A_i)$ via the computed encryption key SK_{ut}. Finally, the smart card transmits $\{C_{ut}, Auth_{ut}\}$ to the trusted server *TS*.

4.3 Authentication and Key Agreement Phase

In this phase, the patient U_i, the trusted server *TS*, and the medical server *MS* achieve fast authentication and key negotiation. The specific steps are as follows, and the detailed process is shown in Fig. 2.

*Step A*1. After receiving the message $\{C_{ut}, Auth_{ut}\}$, the trusted server *TS* decrypts the message C_{ut} using its master key k_1 to obtain $M_1^{'}$, $r_2^{'}$ and $P^{'}$. Then, the *TS* computes $M_1^{'} \oplus ID_t$ to get the patient's identity $ID_i^{'}$. After that, it can construct the encryption key $SK_{ut} = h(ID_i^{'}||ID_t||k_1||r_2^{'})$ using the computed user's identity, the decryption information $r_2^{'}$ and its master key k_1 and identity ID_t. Then the trusted server *TS* can decrypt the authentication $Auth_{ut}$ via the computed encryption key SK_{ut} to obtain $X_1^{'}$, $ID_m^{'}$ and $A_i^{'}$. Then, the trusted server *TS* calculates $X_1^{'} \oplus h(ID_i^{'}||C_{ut}||A_i^{'})$ to get secret high entropy random $m^{'}$. Afterwards, it computes A_i^* =$h(ID_i^{'}||(m^{'} \oplus ID_m^{'})) \oplus P^{'}$ using the decryption message $P^{'}$ hiding in the message C_{ut}. Then it checks the matching difference value between the decryption $A_i^{'}$ and the computed A_i^* is beyond a predefined threshold. If the matching difference value $\Delta(A_i^{'}, A_i^*)$ is beyond a predefined threshold, the trusted server *TS* stops this session. Otherwise, it computes messages $M_2 = h_{bio}(ID_i^{'} \oplus m^{'} \oplus A_i^*)$ and $X_2 = ID_i^{'} \oplus A_i^{'} \oplus m^{'} \oplus ID_m^{'}$ to construct authentication message $Auth_{tm} = E_{SK_{tm}}(M_2||X_2)$ using the pre-shared session key SK_{tm} hold by the trusted server and the medical server. Next, the trusted server *TS* sends $\{Auth_{tm}\}$ to the *MS*.

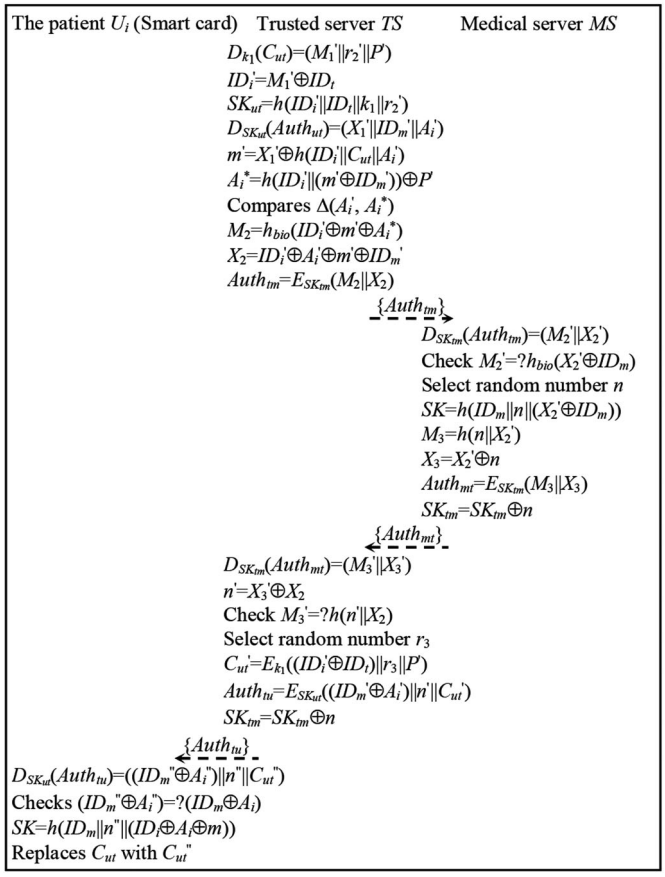


Fig. 2. The authentication and key agreement phase.

*Step A*2. Upon receiving the message $\{Auth_{tm}\}$, the *MS* decrypts the received message $\{Auth_{tm}\}$ using the pre-shared session key SK_{tm} shared by *TS* and *MS* to get information $M_2^{'}$ and $X_2^{'}$. Then, the medical server *MS* computes $h_{bio}(X_2^{'} \oplus ID_m)$ using its identity ID_m and the decryption message $X_2^{'}$. After that, it verifies whether $M_2^{'} = h_{bio}(X_2^{'} \oplus ID_m)$ hold. If not, the medical server *MS* aborts this session. Otherwise, it selects a high entropy random integer n, and calculates the session key $SK = h(ID_m||n||(X_2^{'} \oplus ID_m))$ and the authentication message $Auth_{mt} = E_{SK_{tm}}(M_3||X_3)$ where $M_3 = h(n||X_2^{'})$ and $X_3 = X_2^{'} \oplus n$. After that, the medical server *MS* updates SK_{tm} as $SK_{tm} \oplus n$ and sends authentication message $\{Auth_{mt}\}$ to *TS*.

*Step A*3. When receiving the authentication message $\{Auth_{mt}\}$, the trusted server *TS* first decrypts the $Auth_{mt}$ using the pre-shared session key SK_{tm} to get secret information $M_3^{'}$ and $X_3^{'}$. Then, it computes $n^{'}$=$X_3^{'} \oplus X_2$ and checks whether $M_3^{'}$=$h(n^{'}||X_2)$ hold. If the two values are not equal, the trusted server *TS* aborts this session. Otherwise, the *TS* chooses a high entropy random integer r_3, and updates $C_{ut}^{'}$ as new $C_{ut}^{'}$=$E_{k_1}(ID_i^{'} \oplus ID_t||r_3||P^{'})$. Next, the *TS* constructs an authentication message $Auth_{tu}$=$E_{SK_{ut}}((ID_m^{'} \oplus A_i^{'})||n^{rsquo;}||C_{ut}^{'})$ and set the pre-shared session key SK_{tm}=$SK_{tm} \oplus n^{rsquo;}$. Finally, it sends the message $\{Auth_{tu}\}$ to U_i.

*Step A*4. Upon receiving the message $\{Auth_{tu}\}$, the U_i decrypts the $Auth_{tu}$ via SK_{ut} to obtain $ID_m^{''} \oplus A_i^{''}$, $n^{''}$ and

Authorized licensed use limited to: China University of Geosciences Wuhan Campus. Downloaded on September 06,2023 at 06:15:52 UTC from IEEE Xplore. Restrictions apply.

Cut''. Then the patient U_i checks whether the values of the decrypted information $ID''_m \oplus A''_i$ is equal to the computed values $ID_m \oplus A_i$. If the two values are different, the patient U_i stops this session. Otherwise, it calculates the session key $SK = h(ID_m||n''||(ID_i \oplus A_i \oplus m))$ and replaces the C_{ut} with the decrypted message C''_{ut}.

Up to now, the proposed authenticated key agreement scheme has been entirely executed. Next, the patient U_i establishes secure communications with the corresponding medical server *MS* by using the negotiated session key *SK*.

5 Security Analysis

In this section, we first show that our proposed scheme is provably secure in the Random Oracle model [23], [24]. Then we demonstrate that the proposed scheme can meet the security requirements of e-health systems for user anonymity, user untraceability, and biometric protection.

5.1 Security Proof

1) *Semantic Security of the Session Key*

Theorem 1: Suppose $\mathcal{A}$ violates the semantic security of the session key in the proposed scheme with the advantage of $Adv^{ake}(\mathcal{A})$. Then, we have

$$Adv^{ake}(\mathcal{A}) \leq (q_{h_1}^2 + q_{h_2}^2)/2^{l_h} + 2 \cdot q_d/(|D_{id}| \cdot |D_{pw}| \cdot |D_{bio}|)$$

where q_{h_1} and q_{h_2} denote the upper numbers of *Hash* queries in guessing SK_{ut} and SK_{tm}, respectively. q_d represents $\mathcal{A}$'s guessing attempts towards the user.

Proof: The proof is described through a series of game as follows. The notation E_i denotes the event that $\mathcal{A}$ wins game G_i by guessing the hidden value *c* successfully.

Game G_0. This game simulates the scenario that $\mathcal{A}$ guesses the value *c* as soon as the oracle finishes the initialization procedure. By definitions, we have

$$Adv^{ake}(\mathcal{A}) = 2|Pr[E_0] - 1/2|. \quad (1)$$

Game G_1. To increase the chance of winning this game, $\mathcal{A}$ is allowed to query the oracle with *Execute*($\prod_U^i$, $\prod_{TS}$, $\prod_{MS}$) after the initialization, receiving a transcript of the transmitted messages. After that, $\mathcal{A}$ has to query *Test*(sid_U^i) and answer a guessing value. This game simulates eavesdropping attacks in the real world. Compared to game G_0, $\mathcal{A}$ has no advantage since all messages are encrypted. Therefore, we have

$$Pr[E_1] = Pr[E_0]. \quad (2)$$

Game G_2. Compared to game G_1, the simulations of active attacks are performed by querying the *Send* and *Hash* oracles. To deceives legal participants, $\mathcal{A}$ needs to construct fabricate messages and encrypt them by SK_{ut} or SK_{tm}. However, $\mathcal{A}$ has no idea of the correct values of SK_{ut} or SK_{tm}. According to the proposed scheme, SK_{ut}=$N_i \oplus HPW'$=$h(ID'_i||ID_t||k_1||r_2)$ and SK_{tm}=$h(ID_t||ID_m||k_2)$; so $\mathcal{A}$ has to query the *Hash* oracle and uses the returned values as the encryption keys. No collision is found when querying the oracle. According to the birthday paradox, we have

$$Pr[E_2] - Pr[E_1] \leq (q_{h_1}^2 + q_{h_2}^2)/2^{l_h+1}. \quad (3)$$

Game G_3. The difference between this game and game G_2 is that the *Corrupt*($\prod_U^i$) oracle is added to model the attacks on the smart card. Since SK_{ut}=$N_i \oplus HPW'$=$h(ID_i \oplus pw_i \oplus h_{bio}(B_i))$, $\mathcal{A}$ could try every possible combination of ID_i, pw_i and B_i in D_{id}, D_{pw} and D_{bio} . Thus, we have

$$Pr[E_3] - Pr[E_2] \leq q_d/(|D_{id}| \cdot |D_{pw}| \cdot |D_{bio}|). \quad (4)$$

Since all the oracles have been simulated in game G_3, $\mathcal{A}$ still has little advantage to guess value *c*. Therefore, we deduce

$$Pr[E_3] = 1/2. \quad (5)$$

Finally, combining the above five Equations (1), (2), (3), (4), and (5), we conclude that

$$Adv^{ake}(\mathcal{A}) \leq (q_{h_1}^2 + q_{h_2}^2)/2^{l_h} + 2 \cdot q_d/(|D_{id}| \cdot |D_{pw}| \cdot |D_{bio}|).$$

Thus, the proposed scheme provides the semantic security of the session key.

2) *Perfect Forward Secrecy*

Theorem 2: Let q_{d_1} and q_{d_2} denote the numbers of guessing attempts towards SK_{ut} and SK_{tm}, respectively. Suppose $\mathcal{A}$ violates the perfect forward secrecy in our proposed protocol with an advantage of $Adv^{pfs}(\mathcal{A})$. Then, we have

$$Adv^{pfs}(\mathcal{A}) \leq (q_{h_1}^2 + q_{h_2}^2)/2^{l_h} + q_{d_1}/(2^{l_h-1} \cdot |D_{id}| \cdot |D|) + 2 \cdot q_{d_2}/|D|^2$$

Proof: The game G_0, G_1, and G_2 are the same as we described in *Theorem* 1.

Game G_4. The difference between this game and game G_2 is that the adversary $\mathcal{A}$ queries the *Corrupt*($\prod_{TS}$) to model the violation of perfect forward secrecy. Then the oracle returns the secret keys k_1 and k_2. Since SK_{ut} equals to $h(ID_i||ID_t||k_1||r_2)$ and SK_{tm} equals to $h(ID_t||ID_m||k_2)$, $\mathcal{A}$ could try every possible combination of ID_i in D_{id}, ID_t in D, and ID_m in D. Thus, we have

$$Pr[E_4] - Pr[E_2] \leq q_{d_1}/(2^{l_h} \cdot |D_{id}| \cdot |D|) + q_{d_2}/|D|^2. \quad (6)$$

Since all the oracles has been simulated in game G_4, $\mathcal{A}$ still has little advantage to guess value *c*. Therefore, we de-duce

$$Pr[E_4] = 1/2. \quad (7)$$

Finally, combining the Equations (1), (2)(3), (6) and (7), we conclude that

$$Adv^{pfs}(\mathcal{A}) \leq (q_{h_1}^2 + q_{h_2}^2)/2^{l_h} + q_{d_1}/(2^{l_h-1} \cdot |D_{id}| \cdot |D|) + 2 \cdot q_{d_2}/|D|^2.$$

Thus, the proposed scheme provides the perfect forward secrecy.

5.2 Security Requirement Discussion

1) *User Anonymity*. During the login process, the U_i's identity ID_i is embedded in the C_{ut} and authentication messages $Auth_{ut}$. Without the knowledge of trusted server's master key k_1 and the identity ID_t, the adversary cannot use the intercepted message C_{ut} to extract the patient's identity. Furthermore, since the patient's real identity is protected by a hash function, a secure symmetric encryption algorithm, high entropy random integers, and patient's password and

Authorized licensed use limited to: China University of Geosciences Wuhan Campus. Downloaded on September 06,2023 at 06:15:52 UTC from IEEE Xplore. Restrictions apply.

biometric information, the adversary has no ability to get the patient's identity from the authentication message $Auth_{ut}$.

In the authentication process, the patient U_i's identity is contained in authentication messages $Auth_{tm}$, $Auth_{mt}$, and $Auth_{tu}$. However, if an adversary wants to extract the patient's identity ID_i from the authentication message $Auth_{tm}$, he/she needs to obtain the SK_{tm} shared between the *TS* and *MS* successfully and then decrypts the $Auth_{tm}$ to obtain correct X_2 and M_2. Since the shared key SK_{tm} is preload trusted server *TS* and the medical server *MS*, the adversary cannot obtain it using the intercepted messages. Even if the adversary gets the shared key SK_{tm} and extracts the illegal message X_2 and M_2, he/she cannot guess the patient's identity correctly. That is because the identity ID_i is protected by a biohash function in message M_2 and protected by a high entropy random integer, a hash function, the medical server's identity, the patient's password, and biometric information in message X_2. Similarly, without the knowledge of the shared key SK_{tm} and the random integer, the adversary has no ability to obtain the patient's identity from message $Auth_{mt}$. The adversary also cannot extract the patient's identity using the intercepted message $Auth_{tu}$ since the ID_i is protected by a secure hash function, a secure symmetric encryption algorithm, a high entropy random integer, patient's password, and biometric information. Therefore, our scheme achieves user anonymity.

2) *User untraceability.* In our design, every transmitted message changes in each session to prevent the adversary from tracing the origin of the user. In the registration, the transmitted messages C_{ut} will be updated after successful key negotiation and the authentication Authut is different in each authentication process due to the changes of X_1=$h(ID_i||C_{ut}||A_i) \oplus m$ and A_i=$h(ID_i||m \oplus ID_m) \oplus P^{'}$. Since the high entropy integer m is chosen by the patient randomly in each session and the biometrics inputted by the patient are not the same in each scan, the value of A_i changes in different authentication processes. Due to a similar reason, the message X_1 also changes in each session. So, the adversary cannot trace the patient using the authentication $Auth_{ut}$.

In the authentication process, authentication messages $Auth_{tm}$, $Auth_{mt}$, and $Auth_{tu}$ also change in each authentication process. Since the high entropy random integer m and n are different in each session, the transmitted message $Auth_{mt}$ changes in every authentication process. Moreover, the message $Auth_{tm}$ also cannot be traced due to the change of high entropy random number m and the inputted biometrics by the patient in each session. Similarly, the adversary cannot distinguish whether two sessions belong to one patient via the massage $Auth_{tu}$, because the component C_{ut} updates after successful key negotiation, and the component n is randomly chosen by the medical server *MS* in each session. Therefore, the adversary cannot tell whether two sessions originate from the same patient.

3) *Biometrics protection*. In the patient U_i's smart card, the biometric template B_i is protected by a high entropy random integer r_1. Moreover, without the knowledge of the patient's identity ID_i, biometric information B_i^* and password pw_i, the adversary has no ability to obtain the patient's biometric template B_i by computing $B_i = B_{ir} \oplus R \oplus h(ID_i||h_{bio}(B_i^*)||pw_i)$ via the messages $\{B_{ir}, R\}$ stored in the smart card. Here B_i^* is patient's inputted biometric information and the biohash function $h_{bio}(\cdot)$ outputs the same string for the input biometrics with tolerable changes. Therefore, even if the adversary obtains patient's identity ID_i and password pw_i, he/she still cannot extract the patient's biometric template without knowing the patient's biometric information.

In the proposed scheme, the biometric information is also secure throughout the authentication process. That is because the patient's biometric information embedded in the transmitted messages is protected by hash functions, secure symmetric encryption algorithms, and high entropy random integers. More importantly, in our scheme, the trusted server can verify the patient's biometric information without knowing the patient's biometric value. That is to say, even the trusted server doesn't know the patient's biometric information. Therefore, our scheme provides biometrics protection both in storage and transmission.

TABLE 3
The Functionality Comparisons of Related Schemes

Security attributes	[12]	[13]	[15]	Ours
Replay attacks	Y	Y	Y	Y
Man-in-the-middle attacks	Y	Y	Y	Y
Password guessing attacks	Y	Y	N	Y
Impersonation attacks	Y	Y	Y	Y
DoS attacks	-	N	Y	Y
Smart card theft attacks	Y	N	-	Y
User anonymity	Y	N	N	Y
Untraceability	N	N	N	Y
No clock synchronization	-	Y	-	Y
No verification table	Y	Y	Y	Y
Perfect forward secrecy	Y	Y	N	Y
Known-key security	Y	Y	Y	Y
Session key security	Y	Y	Y	Y
Biometrics protection	Y	-	-	Y

−: Does not implemented or not proved.

6 Performance Analysis

In this section, our work is compared with other related schemes [12], [13], [15] in terms of functionality and computational cost. As illustrated in Table 3, our scheme is proved to be secure against various known attacks and satisfies more security requirements, in comparison with other related schemes [12], [13], [15]. Especially, the proposed scheme realizes privacy protection by introducing biometric template authentication factor and providing the user anonymity, which are very important for practical application in e-health environments.

The user's privacy information is sensitive, so ensuring user untraceability and anonymity are quite critical. However, Yang's scheme [13] and Amin's scheme [15] fails to satisfy the user anonymity and user untraceability; and Sahoo's design [12] cannot provide user untraceability. Besides, Yang's scheme [13] cannot withstand the DoS attacks and smart card theft attacks; Amin's scheme [15] doesn't achieve perfect forward secrecy and suffers from the offline password guessing attack. According to Table 3, our scheme achieves more security requirements, and is secure against

Authorized licensed use limited to: China University of Geosciences Wuhan Campus. Downloaded on September 06,2023 at 06:15:52 UTC from IEEE Xplore. Restrictions apply.

Fig. 3. Raspberry Pi 3B+.

various known attacks, in comparison with Sahoo's scheme [12], Yang's scheme [13], and Amin's scheme [15].

Next, we compare the computational cost of our scheme and the current schemes [12], [13], [15]. Note that string concatenation operation and exclusive-or operation are negligible in our evaluating process. Some notations are defined as follows:

T_e/T_d: The time for executing a symmetric key encryption/decryption operation.

T_h: The time for executing a one-way hash function operation.

T_{bh}: The time for executing a biohash algorithm operation.

T_m: The time for executing a point multiplication operation on the elliptic curve.

In our experiment, we adopted Raspberry Pi as shown in Fig. 3 as a low energy medical sensor device to simulate the e-health environment. The proposed scheme and the related schemes [12], [13], [15] are implemented on the following devices. The first one is a Raspberry Pi 3 Model B+ with a 64-bit quad-core Broadcom Arm Cortex A53 architecture processor clocked at 1.4 GHz and a memory size of 1.00 GB, which can be considered as a client or bio-sensor (*BS*), followed by an i7-4720HQ processor equipped with a Dell laptop clocked at 2.60 GHz with 8 GB of RAM and 64-bit Windows 10 operating system, acting as a server, medical server (*MS*) or sensor node. And a personal computer, a Dell laptop with a Pentium-G850 processor clocked at 2.9 GHz, 4 GB of RAM, and a 64-bit Windows 10 operating system. Its role in the system is as a Trusted Server (*TS*), sensor as well as Gateway Node (*GWN*). OpenSSL and C++ are the main external programming libraries in this work, and OpenSSL built-in functions are chosen as the main source of programming algorithms. Furthermore, we adopted a super singular elliptic curve on a 160-bit finite field to reach the same security level as the 1024-bits RSA algorithm.

TABLE 4
Comparison of Computational Cost

	[12]	[13]	[15]	Ours
MD/*User*	$8T_h + 3T_m$ $+1T_e + 1T_d$ ≈2.159ms	$20T_h$ ≈1.342ms	$12T_h$ ≈1.206ms	$1T_{bh} + 5T_h$ $+1T_e + 1T_d$ ≈0.314ms
GWN/*Sensor*/*TS*	$4T_h + 2T_m$ $+1T_e + 1T_d$ ≈0.824ms	$17T_h$ ≈0.079ms	$19T_h$ ≈0.093ms	$1T_{bh} + 4T_h$ $+3T_e + 3T_d$ ≈0.042ms
GW/*Sensor*/*MS*	$3T_h + 2T_m$ $+1T_e + 1T_d$ ≈0.692ms	$21T_h$ ≈0.096ms	$6T_h$ ≈0.041ms	$1T_{bh} + 2T_h$ $+1T_e + 1T_d$ ≈0.016ms
Total	$15T_h + 7T_m$ $+3T_e + 3T_d$ ≈3.675ms	$58T_h$ ≈1.517ms	$37T_h$ ≈1.34ms	$3T_{bh} + 11T_h$ $+5T_e + 5T_d$ ≈0.372ms

The simulation process involves three participants. They are simulated using the Raspberry Pi and two computers of different configurations. The computational cost and running time among our scheme and other related schemes [12], [13], [15] are compared in Table 4. According to the Table 4, the total execution time of Sahoo's scheme [12] is 3.675ms. Yang's scheme [13] requires executing 1.517ms in total. In Amin *et al.*'s scheme [15], the total execution time is 1.34ms. In our proposed scheme, the actual simulation time at the user side, the trusted server side and the medical server side is 0.314ms, 0.042ms and 0.016ms, respectively. Compared to Sahoo's scheme [12], Yang's scheme [13] and Amin's scheme [15], the proposed scheme reduces the computational cost up to 89.9%, 75.4% and 72.2% respectively. Furthermore, compared to the related schemes [12], [13], [15], our scheme achieves higher security. So, our proposed authentication is more suitable for e-health environments compared to the state-of-the-art authentication schemes [12], [13], [15].

TABLE 5
Comparison of Communication Cost

	[12]	[13]	[15]	ours
Costs(bits)	2656	3072	2080	1220
Number of messages	4	8	5	3

The comparison of communication cost between our proposed scheme and other three related schemes is shown in Table 5. In our experiment, the timestamp and the user identity are 32 bits and 64 bits, respectively. The output of the hash function is 160 bits, and a point of elliptic curve is 320 bits. The output of the biohash function is determined by the security parameter and the input biometric feature. In addition, the output of a 256-bit AES is based on the input of the plaintext. As shown in Table 5, our proposed scheme has the smallest communication cost which is 1220 bits and requires only 3 messages. The communication costs of the other three related schemes [12], [13], [15] are 2656 bits, 3072 bits, and 2080 bits, respectively, and the number of messages is 4, 8, and 5, respectively. Compared with related schemes [12], [13], [15], our proposed scheme reduces the communication cost and the number of messages.

7 Conclusion

In this paper, we presented a fast three-factor authentication and key agreement scheme with privacy protection using three factors for e-health systems. The biometrics integrated with smart cards and passwords are utilized to achieve mutual authentication, user anonymity, user untraceability, and biometric protection. Furthermore, the security and performance of our scheme were evaluated to demonstrate utility. One future extension is to design a secure communication mechanism via a shared session key to facilitate the secure transmission of biomedical signals in practical settings.

Authorized licensed use limited to: China University of Geosciences Wuhan Campus. Downloaded on September 06,2023 at 06:15:52 UTC from IEEE Xplore. Restrictions apply.

REFERENCES

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

[2] W. Tang, K. Zhang, J. Ren, Y. Zhang, and X. Shen, "Flexible and efficient authenticated key agreement scheme for bans based on physiological features," *IEEE Trans. Mobile Comput.*, vol. 18, no. 4, pp. 845–856, Apr. 2019.

[3] X. Luo, J. Sun, Z. Wang, S. Li, and M. Shang, "Symmetric and nonnegative latent factor models for undirected, high dimensional and sparse networks in industrial applications," *IEEE Trans. Ind. Electron.*, vol. 13, no. 6, pp. 3098–3107, Dec. 2017.

[4] Z. Mehmood, A. Ghani, G. Chen, and A. S. Alghamdi, "Authentication and secure key management in e-health services: A robust and efficient protocol using biometrics," *IEEE Access*, vol. 7, pp. 113385–113397, 2019.

[5] A. Abuadbba and I. Khalil, "Walsh–Hadamard-based 3-D steganography for protecting sensitive information in point-of-care," *IEEE Trans. Biomed. Eng.*, vol. 64, no. 9, pp. 2186–2195, Sep. 2017.

[6] D. Wang and P. Wang, "Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks," *Ad Hoc Netw.*, vol. 20, no. 2, pp. 1–15, 2014.

[7] S. F. Aghili, H. Mala, M. Shojafar, and P. Peris-Lopez, "LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for E-health systems in IoT," *Future Gener. Comput. Syst.*, vol. 96, pp. 410–424, 2019.

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

[9] J. L. Hou and K. H. Yeh, "Novel authentication schemes for IoT based healthcare systems," *Int. J. Distrib. Sensor Netw.*, vol. 2015, pp. 1–9, 2015.

[10] C. T. Li, C. C. Lee, C. Y. Weng, and S. J. Chen, "A secure dynamic identity and chaotic maps based user authentication and key agreement scheme for e-healthcare systems," *J. Med. Syst.*, vol. 40, no. 11, 2016, Art. no. 233.

[11] N. Ravanbakhsh and M. Nazari, "An efficient improvement remote user mutual authentication and session key agreement scheme for e-health care systems," *Multimedia Tools Appl.*, vol. 77, no. 11, pp. 55–88, 2018.

[12] S. S. Sahoo, S. Mohanty, and B. Majhi, "A secure three factor based authentication scheme for health care systems using IoT enabled devices," *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 15, pp. 1419–1434, 2020.

[13] Z. Yang, J. Lai, Y. Sun, and J. Zhou, "A novel authenticated key agreement protocol with dynamic credential for WSNs," *ACM Trans. Sensor Netw.*, vol. 15, no. 2, pp. 22.1–22.27, 2019.

[14] F. Wu *et al.*, "A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks," *Future Gener. Comput. Syst.*, vol. 82, no. MAY, pp. 727–737, 2017.

[15] 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 Gener. Comput. Syst.*, vol. 80, pp. 483–495, 2018.

[16] G. Ankur, T. Meenakshi, and S. Aakar, "A provably secure and efficient anonymous mutual authentication and key agreement protocol for wearable devices in WBAN," *Comput. Commun.*, vol. 160, pp. 311–325, 2020.

[17] A. M. Almuhaideb and K. S. Alqudaihi, "A lightweight and secure anonymity preserving protocol for WBAN," *IEEE Access*, vol. 8, pp. 178183–178194, 2020.

[18] A. K. Das, "A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor," *Int. J. Commun. Syst.*, vol. 30, no. 1, 2017, Art. no. e2933.

[19] F. Wu, "An improved and provably secure three-factor user authentication scheme for wireless sensor networks," *Peer-to-Peer Netw. Appl.*, pp. 1–20, 2016.

[20] 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.

[21] K. Chatterjee, "An improved authentication protocol for wireless body sensor networks applied in healthcare applications," *Wireless Pers. Commun.*, vol. 111, no. 4, pp. 2605–2623, 2020.

[22] A. Jabbari and J. Mohasefi, "Improvement of a user authentication scheme for wireless sensor networks based on Internet of Things security," *Wireless Pers. Commun.*, vol. 116, pp. 2565–2591, 2020.

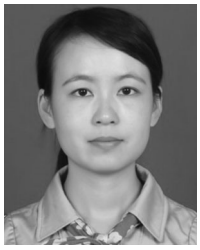
[23] M. Abdalla, P. A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proc. Int. Workshop Public Key Cryptogr.*, 2005, pp. 64–84.

[24] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in *Proc. 19th Int. Conf. Theory Appl. Cryptogr. Techn.*, 2000, pp. 139–155.

[25] A. Lumini and L. Nanni, "An improved biohashing for human authentication," *Pattern Recognit.*, vol. 40, no. 3, pp. 1057–1065, 2007.

[26] M. Wang, K. He, J. Chen, Z. Li, W. Zhao, and R. Du, "Biometrics-authenticated key exchange for secure messaging," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2021, pp. 2618–2631.

[27] G. L. Hammad and K. Wang, "Cancelable biometric authentication system based on ECG," *Multimedia Tools Appl.*, vol. 78, no. 2, pp. 1857–1887, 2019.



Liping Zhang received the PhD degree in information security from the Huazhong University of Science and Technology in 2009. She is currently an associate professor of information and network security with the China University of Geosciences. She has authored or coauthored more than 30 research papers, most of which are refereed international journal papers, including IEEE/ACM/IET journal papers. Her research interests include network security, key management and distribution, and privacy protection. She is the principal grant holder of three externally funded research projects.

Yue Zhu received the BSc degree in information security from the China University of Mining and Technology, Xuzhou, China, in 2019. She is currently working toward the master's degree in computer technology with the China University of Geosciences, Wuhan, China. Her research interests include communications security and network security.

Wei Ren (Member, IEEE) received the PhD degree in computer science from the Huazhong University of Science and Technology, China. He is currently a full Professor with the School of Computer Science, China University of Geosciences, Wuhan, China. He was with the Department of Electrical and Computer Engineering, Illinois Institute of Technology, USA, in 2007 and 2008, the School of Computer Science, University of Nevada Las Vegas, USA, in 2006 and 2007, and the Department of Computer Science, The Hong Kong University of Science and Technology, in 2004 and 2005. He has authored or coauthored more than 100 refereed papers, one monograph, and four textbooks. He has obtained ten patents and five innovation awards. He is a distinguished member of the China Computer Federation.

Authorized licensed use limited to: China University of Geosciences Wuhan Campus. Downloaded on September 06,2023 at 06:15:52 UTC from IEEE Xplore. Restrictions apply.

Yixin Zhang received the MS degree in information security from the School of Computer Science, China University of Geosciences in 2019. She is currently working toward the PhD degree in information security. Her research interests include communications security, blockchain, and cryptanalysis.

Kim-Kwang Raymond Choo (Senior Member, IEEE) received the PhD degree in information security from the Queensland University of Technology, Australia, in 2006. He is currently holds the cloud technology endowed professorship with The University of Texas at San Antonio. He is the founding co-editor-in-chief of ACM Distributed Ledger Technologies: Research & Practice, and the founding chair of IEEE TEMS Technical Committee on Blockchain and Distributed Ledger Technologies. He is an ACM distinguished speaker and IEEE computer society distinguished visitor (2021–2023), and a web of science's highly cited researcher (Computer Science- 2021, Cross-Field-2020). In 2015, he and his team won the Digital Forensics Research Challenge organized by the Germany's University of Erlangen-Nuremberg. He was the recipient of the 2019 IEEE Technical Committee on Scalable Computing Award for Excellence in Scalable Computing (Middle Career Researcher), British Computer Society's 2019 Wilkes Award Runner-up, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion, and British Computer Society's Wilkes Award in 2008. He was also the recipient of the best paper awards from IEEE Systems Journal in 2021, IEEE DSC 2021, IEEE Computer Society's Bio-Inspired Computing STC Outstanding Paper Award for 2021, IEEE Consumer Electronics Magazine for 2020, Journal of Network and Computer Applications for 2020, EURASIP Journal on Wireless Communications and Networking in 2019, IEEE TrustCom 2018, and ESORICS 2015, the IEEE Blockchain 2019 Outstanding Paper Award; and best student paper awards from Inscrypt 2019 and ACISP 2005.

▷ **For more information on this or any other computing topic, please visit our Digital Library at** www.computer.org/csdl.

Authorized licensed use limited to: China University of Geosciences Wuhan Campus. Downloaded on September 06,2023 at 06:15:52 UTC from IEEE Xplore. Restrictions apply.