Privacy Protection for E-Health Systems by Means of Dynamic Authentication and Three-Factor Key Agreement

Liping Zhang, Yixin Zhang, Shanyu Tang, *Senior Member, IEEE*, and He Luo

***Abstract*—During the past decade, the electronic healthcare (e-health) system has been evolved into a more patient-oriented service with smaller and smarter wireless devices. However, these convenient smart devices have limited computing capacity and memory size, which makes it harder to protect the user's massive private data in the e-health system. Although some works have established a secure session key between the user and the medical server, the weaknesses still exist in preserving the anonymity with low energy consumption. Moreover, the misuse of biometric information in key agreement process may lead to privacy disclosure, which is irreparable. In this study, we design a dynamic privacy protection mechanism offering the biometric authentication at the server side whereas the exact value of the biometric template remains unknown to the server. And the user anonymity can be fully preserved during the authentication and key negotiation process because the messages transmitted with the proposed scheme are untraceable. Furthermore, the proposed scheme is proved to be semantic secure under the real-or-random model. The performance analysis shows that the proposed scheme suits the e-health environment at the aspect of security and resource occupation.**

***Index Terms*—Authentication, electronic healthcare (e-health) system, key agreement, privacy protection.**

I. Introduction

ELECTRONIC healthcare (e-health) systems are getting increasingly popular in moving patients from hospital ward rooms into their homes. Many applications such as home health monitoring and personal health records (PHRs) are developed in order to manage chronic diseases and enable patients' self-care. During the last decade, Internet-capable terminals with smaller size have been replacing the old-fashioned desktops and medical equipment. Various handhold and wearable devices (e.g., tablets, smart watches, and smart bands) may act as communicators, sensors, and monitors with the advances in Internet of Things technologies [1]. Usually, these devices are deployed on a patient's body or in surrounding environment collecting real-time data, transmitting them to the remote server, and then to the clients. Diagnoses and emergency decisions can be made according to the received information and the personal electronic health records. In the e-health systems, for example, a patient suffering from a cardiac disease is equipped with a number of small sensors on her/his body to monitor some vital signs such as heart rate, blood pressure, blood oxygen level, etc. The medical sensors collect the physical data and then transmit them to a medical server. After receiving the physical data, the medical server establishes a PHR for each patient. So, the doctor checks the patient's PHR and gives a more accurate diagnosis for the patient according to the PHR and the continuous monitoring data collected by the sensors. Through the e-health system, the patients can enjoy the health care and medical treatment timely at home. Moreover, emergency circumstances such as a heart attack can be detected quickly and the patient's life can be saved.

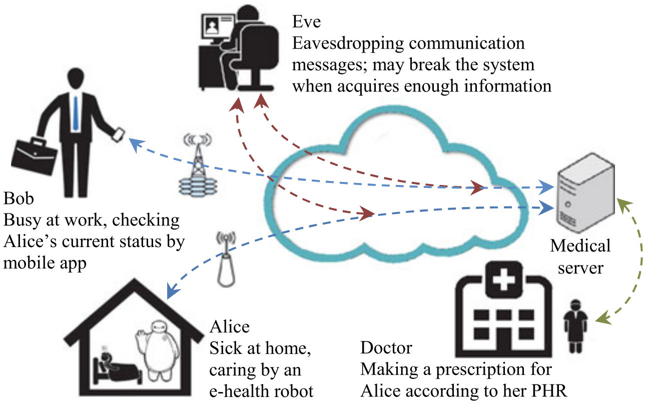

Eve
Eavesdropping communication messages; may break the system when acquires enough information
Bob
Busy at work, checking Alice's current status by mobile app
Medical server
Alice
Sick at home, caring by an e-health robot
Doctor
Making a prescription for Alice according to her PHR

Fig. 1. Application scenario and the potential attacks of the e-health.

However, the natural defect of wireless communications raises a big concern about privacy preserving in e-health services. As shown in Fig. 1, most of the entities in the system are connected to each other wirelessly where the adversaries may extract numerous useful information by passive attacks. Tracing the origin of data is one of these means, which are easily overlooked. Generally speaking, the user's location can be acquired and the login time and frequency can be derived immediately. Combined with some information by googling that particular

Manuscript received February 17, 2017; revised April 27, 2017 and June 23, 2017; accepted July 11, 2017. Date of publication August 14, 2017; date of current version December 15, 2017. This work was supported by the National Natural Science Foundation of China under Grant 61303237 and Grant 61272469. *(Corresponding author: Liping Zhang.)*

L. Zhang, Y. Zhang, and H. Luo are with the School of Computer Science, China University of Geosciences, Wuhan 430074, China (e-mail: carolyn321@163.com; ss.fc.xyz@163.com; rabbit_cug@163.com).

S. Tang is with the School of Computing and Engineering, University of West London, London, W5 5RF, U.K. (e-mail: shanyu.tang@gmail.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIE.2017.2739683

place, it is easy to conclude the user's job, work place, home address, and much other information, which largely reduces the difficulty of guessing the real identity and the correct password of the user. And when the least expected thing happens, unauthorized adversaries may get access to the patient's current health condition, medical history, and other binding information such as mobile phone number and credit card number. The patient will suffer much more than the illness itself. Considering the worst condition, if the adversary has an attempt at harming the patient, she/he may modify the patient's vital health information. And when these modified messages are transmitted to doctors, wrong prescription can be made and the patient's life may be threatened.

Since medical data are transmitted and exposed to the unsecured public network, the patients' privacy is susceptible to several attacks [2]. To deal with this situation, authenticated key agreement schemes have been applied to provide mutual authentication and session key negotiation between the authorized user and the server with various technologies [3]–[8]. And the shared session key can be used to encrypt/decrypt the medical information over the public network to ensure the confidentiality and integrity of the data communications in an e-health system.

In order to construct a secure session key as required, some key agreement schemes have been proposed [3]–[5]. Yoon and Yoo employed elliptic curve cryptography (ECC) to generate a shared session key [3]. Based on Chebyshev chaotic maps, Farash and Attari's scheme [4] achieved mutual authentication and key agreement between the user and the server. Das *et al*. applied passwords and smart cards to design a two-factor key agreement scheme with the help of hash functions [5]. However in 2014, two-factor key agreement schemes without adopting asymmetric primitives were proved to be not privacy-preserving, as they were unable to preserve the user anonymity [9]. Furthermore, if the user's password is verified with a related value in the smart card, these schemes are subject to smart card breach attacks [9]. Since user anonymity including the untraceability is not considered or not provided in the above-mentioned schemes [3]–[5], these key agreement schemes are not suitable for e-health systems.

To achieve privacy-preserving in designing an authenticated key agreement scheme, one solution is applying public-key mechanisms. Li *et al*. adopted ECC to construct a key agreement scheme with user anonymity and the untraceability by using the technology of smart cards [6]. Tsai *et al.* also proposed a privacy preserving authentication scheme based on ECC [7], which was an improvement of Li *et al*.'s scheme [6]. Although both schemes realize user anonymity and the untraceability, they are not suitable for an e-health circumstance due to the usage of time-consuming operations such as the scalar multiplication and the point addition of an elliptic curve. And the smart sensors deployed in the e-health system cannot afford the large power consumption at the aspect of computation and communication, especially the wearable devices and implanted smart chips. So, the time-consuming operations should be avoided in the design of authenticated key agreement schemes for an e-health system. In addition, Li *et al*.'s scheme [6] and Tsai *et al*.'s scheme [7] both suffered from the smart card loss attack.

Another approach is to perform a symmetric three-factor authentication, which means adding a step of matching biometric features to the scheme. Amin *et al.* [8] took a step in designing a secure three-factor key agreement scheme using biometrics, passwords, and smartcards for e-health systems. Their scheme is efficient since only hash functions and biohash functions are involved. Though their scheme employs random numbers and biohash functions to achieve user anonymity, it fails to provide the untraceability. In theory, a lightweight three-factor key agreement scheme could be adaptable to the e-health system environment better with the help of biohash technology. However, the usage of the biometrics should be more careful in some existing schemes [3], [10]–[16] since the leakage of the biometrics could lead to more security problems. Moreover, it is also known that the biometric characteristics are not like passwords that can be changed at will. Once the biometric template is revealed, the damage to user's privacy is irreparable.

In 2009, Fan and Lin proposed an idea of truly three-factor authentication [17]. Their studies showed that the biometric characteristics should be verified at the server side rather than at the user's smart card while the exact value of the biometric information remains unknown to the server. However, this idea is not easy to achieve. The difficulty lies not only in the aforementioned verification process, but also in the transmission forms of the biometric information to make sure that even if the adversary controls the entire communication channel, she/he is unlikely to obtain the user's real identity or to find the connection between any two messages.

In this study, we present a practical authenticated key agreement scheme, which can meet the security needs and the computational demands of e-health systems. We focus on solving the aforesaid problems in biometric authentication and key negotiation process and providing the user's privacy effectively and efficiently. The main contributions of our work are described as follows.

Secure biometric authentication on the server: In our proposed scheme, the medical server is responsible for checking the user's validity. To prevent the server from knowing the biometric template, a random string is combined with it using the exclusive-or operation and then the two masked strings are matched at the server side instead of matching the real template with the biometric characteristic. Besides, all these masked strings are protected by hash or biohash functions during the authentication and key negotiation process. Thus, the medical server can verify the biometric characteristics without storing and obtaining the exact values in our design.

Strong privacy protection: In the storage devices such as smart cards and the database, the biometric templates are protected by random numbers, which makes sure that only the user has the possession of the real value. Aiming at anonymity and untraceability, a dynamic mechanism is proposed to break the linkage of the transmitted messages. The relevant values in the database and the smart card will be updated after each successful login. Furthermore, we have proved our scheme to be semantic secure under real-or-random model.

Efficiency: The proposed scheme is lightweight since only hash functions and biohash functions are adopted during the whole procedure. In addition, no verification process needs to be performed at the user side, which reduces the redundancy in the authentication process.

The rest of our paper is organized as follows. Section II introduces the related work including a brief development history and some common mistakes in designing three-factor authentication schemes. We describe the detail of our proposed scheme in Section III and prove it to be secure under the real-or-random model in Section IV. Section V shows the evaluation result of the proposed scheme. The paper is concluded in Section VI.

II. Related Work

Public key cryptography has already been applied to control the access to the remote healthcare server. Three-factor schemes based on discrete logarithm problem [18], [19], extended chaotic maps [4], [10], [20], and bilinear pairing [11] have been proposed regardless of large computational cost. To reduce the execution time, many schemes based on ECC [3], [6], [7], [21]–[24] have been suggested. In 2009, Fan and Lin [17] proposed a three-factor authentication scheme using both asymmetric and symmetric cryptosystems which could meet most security needs. But Yeh *et al.* [21] showed that Fan and Lin's scheme could not resist the insider attack and presented a new three-factor scheme based on elliptic curve discrete logarithm problem. Unfortunately, Wu *et al.* [23] found some weaknesses in Yeh *et al.*'s scheme, such as useless user identity, no session key, no mutual authentication, and suffering from impersonation attacks. And then they proposed another new scheme. Although these schemes have been improved gradually with better security and efficiency [24], the cost is still not low enough for the mobile devices and the smart chips, which are widely deployed in e-health systems.

To solve this problem, many schemes adopted one-way hash functions to improve the efficiency [12]–[16], [25], [26]. However, design flaws occurred more frequently in hash-based schemes than asymmetric ones. In 2010, Li and Hwang [12] proposed a three-factor authentication scheme by applying only hash functions. Soon after their publication, Li *et al.* [13] pointed out that the man-in-the-middle attack existed in their scheme. Later on, Das [14] claimed that Li and Hwang's scheme had some disadvantages and then presented a new biometric-based scheme. Li *et al.*'s scheme was also improved by Das [14] for lack of password updating phase. However, An [15] pointed out that Das's scheme suffered from the insider attack, the password guessing attack, and the impersonation attack. An also presented an improved scheme. Unfortunately, Khan and Kumari [16] demonstrated that An's scheme was vulnerable to the password guessing attack and other security failures occurred such as lack of mutual authentication and user anonymity. Recently, some solutions using biohash functions have been proposed to balance the contradictory of security and efficiency in e-health systems [25], [26]. As only hash function and biohash function are involved, these schemes achieve high performance.

In 2014, Wang and Wang [9] proved that the two-factor schemes adopting symmetric algorithms failed to preserve user anonymity. Additionally, they drew a conclusion that smart card breach attacks may break the entire system if the verification value is stored in the smart card. Through rigorous analysis, biometric features could be used to solve the problem. Many attempts have been proposed involving three-factor authentication techniques [3], [10]–[16]. But this method is not easy to accomplish. During our study of existing three-factor schemes, we witnessed many common misuses of biometric information. For example, great hidden hazards exist because the biometric template is stored in the smart card or transmitted on an insecure channel without any protection [3], [10]. If the smart card is obtained by an adversary, the biometric template can be easily extracted by side-channel attacks or reverse engineering. The transmitted biometric data can be obtained by eavesdropping the communication channel. In some schemes, biometric information is used as a part of the input of a hash function [11]–[16]. In this situation, valid biometric data cannot pass the verification process unless they are exactly the same with the template in a tiny probability. Thus, these schemes cannot be put into practice.

In fact, these misuses can be avoided by applying biohash functions into the scheme. The biohash function is designed to map an individual's biometric feature to a specific binary string that has a tolerance of noise [27], [28]. It means that if the inputs are not exactly the same but in a bearable threshold, the outputs of the biohash function will be equal. Also, the biohash function holds one-way property like the hash function. There are many ideas proposed in the literature, such as error-correcting codes [29], fuzzy commitments [30], fuzzy extractors [27], [31], and fuzzy vaults [32], [33]. These algorithms have already been referenced in newly presented key agreement schemes. In 2011, Huang *et al.* [34] proposed a generic framework for three-factor authentication using fuzzy extractors. They claimed that their scheme could provide secure three-factor authentication and preserve user privacy. Later in 2014, Yu *et al.* [35] presented an improvement of Huang *et al.*'s framework by applying fuzzy vaults. More efficiency and practicality have been achieved in their approach; and they proved their scheme in the random oracle model.

Apparently, applying biohash functions is just a proper way of using biometric information in the scheme. Some biohash-based authentication schemes cannot solve the problems of suffering the smart card breach attack and not providing the user anonymity [3], [10]–[16]. After analyzing the existing schemes, we draw a conclusion that the weakness lies in verifying biometric information stored in the smart card rather than on the server. Thus, the server has no idea about whether the verification is performed correctly. In addition, the user's anonymity including untraceability should be protected to provide strong privacy protection. If the adversary breaks into a database containing the user's biometric templates, these data can be used as a dictionary to break other systems with similar structure. Although the biometric database is not revealed on a large scale such as the identity and password databases, a prevention step should be taken before it really happens.

III. Our Proposed Scheme

Since our scheme only adopts hash functions and biohash functions, extra steps should be taken to meet the security needs

TABLE I
NOTATIONS USED IN THIS PAPER

Notation	Description
U_i	The ith user (could be a patient, a doctor, or a relative) participates in a phase
S	The medical server of the e-health system
$\mathrm{ID}_i, \mathrm{PW}_i$	The identity and the password of U_i
T_i, B_i	The biometric template and the biometric data of U_i
s	The master key of the medical server
$\mathrm{ID}_{\mathrm{SC}}$	The identity of the smart card
r_x	High-entropy random numbers
C_j	The jth transmitted value in this scheme
$h(\cdot)$	A collision free hash function
$h_{\mathrm{Bio}}(\cdot)$	A secure biohash function
Δ	A matching algorithm of biometrics
$\oplus$	The exclusive-or operation
$\|$	The concatenation operation
$f(\cdot)$	Dynamic strings generating algorithm

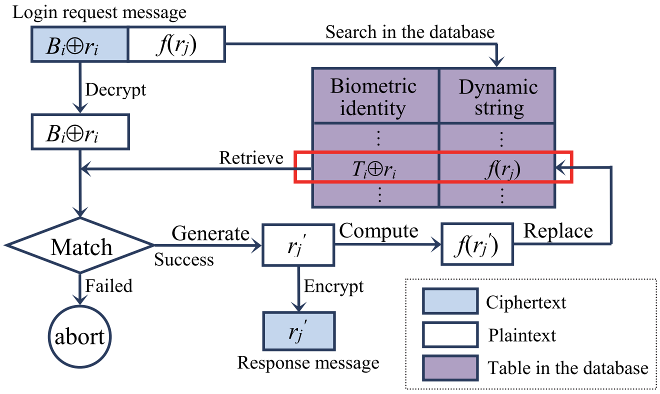


Fig. 2. Biometric authentication process on the server in our proposed scheme.

of e-health systems. In this section, we first introduce a dynamic mechanism in our proposed scheme including a dynamic table maintained on the medical server. After that, the details of the scheme are presented. Some notations are used to describe the scheme clearly, as shown in Table I.

Traditionally, an identity-password table is stored in the remote database offering verification at the server. The login request message usually consists of a pair of the identity and the password or its hash value. After receiving the login message, the server searches for the identity in the database and then compares the corresponding password or the hash value with the receiving string. However, this table structure is likely to suffer from the stolen verifier attack and the insider attack, let alone the violence of the user anonymity and untraceability. To deal with these weaknesses, a dynamic verification table and a new authentication process are presented in our scheme as shown in Fig. 2.

The login request message contains the user's biometric feature B_i which has just been scanned on the remote terminal and combined with the random number r_i (extracted from the smart card) by using an exclusive-or operation. With the help of another random number r_j, a dynamic string generated by a particular algorithm $f(\cdot)$ is also included to locate the corresponding masked biometric template $T_i \oplus r_i$ in the database. Here, $f(\cdot)$ is a one-way and collision-free algorithm. Then, the server matches two masked strings $B_i \oplus r_i$ and $T_i \oplus r_i$. If the result is beyond a bearable threshold, the server aborts the session. Otherwise, a new random number r_j' is generated for next login and $f(r_j)$ is replaced by $f(r_j')$ in the database. Meanwhile, the smart card updates the random number r_j with r_j'. Note that $B_i \oplus r_i$ in the login request message and r_j' in the response message are not in plaintext during the transmitting process.

In the proposed dynamic mechanism, the user's biometric characteristics are not exposed to the server whereas the verification process can still be performed successfully. Even if the dynamic verification table is stolen, the adversary cannot obtain the biometric templates. Furthermore, a new random number will be generated after every successful login preparing for next conversation. The linkage in the messages that comes from the same user has been greatly reduced due to its randomness. Thus, the users in this mechanism are anonymous and untraceable literally. Next, we describe the details of our proposed dynamic authentication and three-factor key agreement scheme for e-health systems, as shown in Fig. 3.

A. Registration Phase

In order to be a legal member of the system, a new user U_i needs to register with the medical server S by performing the following three steps. Thereafter, the user U_i is issued with a smart card; the medical server S stores the protected biometric information of the user U_i in its database.

Step R1: the user U_i chooses his/her identity ID_i and password PW_i which she/he can remember easily. The terminal device then acquires U_i's biometric data T_i as a template and uses it to compute $C_1 = h(\mathrm{ID}_i||\mathrm{PW}_i||h_{\mathrm{Bio}}(T_i))$. Next, the terminal device masks the user U_i's biometric template T_i with a random integer r_1 by computing $C_2 = T_i \oplus r_1$. Then, the user U_i sends $\{C_1, C_2\}$ as a registration request message to the medical server S in a secure channel.

Step R2: after receiving the registration request from the user U_i, the medical server S combines its master key s with U_i's private information C_2 by calculating $M = h(h_{\mathrm{Bio}}(C_2)||s)$. For the further verification process, the medical server S selects another random integer r_2 and computes $W = h(h_{\mathrm{Bio}}(C_2 \oplus r_2))$, $X = h(\mathrm{ID}_{\mathrm{sc}}||C_1||M) \oplus r_2$, and $Y = M \oplus C_1$. Next, the medical server S stores $\{C_2, W_0, W\}$ in its database where W_0 equals NULL. Then, the medical server S writes $\{\mathrm{ID}_{\mathrm{sc}}, h(\cdot), h_{\mathrm{Bio}}(\cdot), X, Y\}$ into the smart card. And the smart card is delivered to the patient user U_i in a secure way.

Step R3: the user U_i writes $Z = r_1 \oplus h_{\mathrm{Bio}}(T_i)$ into the receiving smart card, thus finishing the registration phase successfully.

B. Login Phase

The user U_i needs to perform the following operations in order to be authenticated by the medical server S when the user U_i wants to get some information from the medical server S.

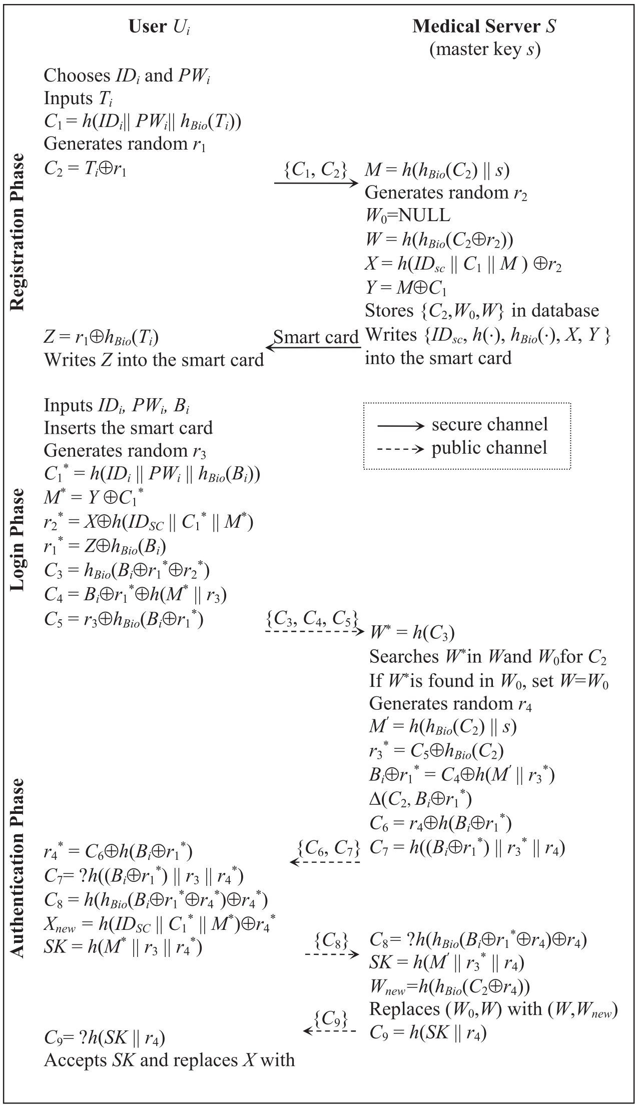

User U_i
Medical Server S
(master key s)
Registration Phase
Chooses ID_i and PW_i
Inputs T_i
$C_1 = h(ID_i \| PW_i \| h_{Bio}(T_i))$
Generates random r_1
$C_2 = T_i \oplus r_1$
$\{C_1, C_2\}$
$M = h(h_{Bio}(C_2) \| s)$
Generates random r_2
W_0=NULL
$W = h(h_{Bio}(C_2 \oplus r_2))$
$X = h(ID_{sc} \| C_1 \| M) \oplus r_2$
$Y = M \oplus C_1$
Stores $\{C_2, W_0, W\}$ in database
$Z = r_1 \oplus h_{Bio}(T_i)$
Writes Z into the smart card
Smart card
Writes $\{ID_{sc}, h(\cdot), h_{Bio}(\cdot), X, Y\}$ into the smart card
Login Phase
Inputs ID_i, PW_i, B_i
Inserts the smart card
Generates random r_3
$C_1^* = h(ID_i \| PW_i \| h_{Bio}(B_i))$
$M^* = Y \oplus C_1^*$
$r_2^* = X \oplus h(ID_{SC} \| C_1^* \| M^*)$
$r_1^* = Z \oplus h_{Bio}(B_i)$
$C_3 = h_{Bio}(B_i \oplus r_1^* \oplus r_2^*)$
$C_4 = B_i \oplus r_1^* \oplus h(M^* \| r_3)$
$C_5 = r_3 \oplus h_{Bio}(B_i \oplus r_1^*)$
secure channel
public channel
$\{C_3, C_4, C_5\}$
Authentication Phase
$W^* = h(C_3)$
Searches W^*in $W$and $W_0$for C_2
If $W^*$is found in W_0, set W=W_0
Generates random r_4
$M' = h(h_{Bio}(C_2) \| s)$
$r_3^* = C_5 \oplus h_{Bio}(C_2)$
$B_i \oplus r_1^* = C_4 \oplus h(M' \| r_3^*)$
$\Delta(C_2, B_i \oplus r_1^*)$
$C_6 = r_4 \oplus h(B_i \oplus r_1^*)$
$C_7 = h((B_i \oplus r_1^*) \| r_3^* \| r_4)$
$\{C_6, C_7\}$
$r_4^* = C_6 \oplus h(B_i \oplus r_1^*)$
$C_7 = ?h((B_i \oplus r_1^*) \| r_3 \| r_4^*)$
$C_8 = h(h_{Bio}(B_i \oplus r_1^* \oplus r_4^*) \oplus r_4^*)$
$X_{new} = h(ID_{SC} \| C_1^* \| M^*) \oplus r_4^*$
$SK = h(M^* \| r_3 \| r_4^*)$
$\{C_8\}$
$C_8 = ?h(h_{Bio}(B_i \oplus r_1^* \oplus r_4) \oplus r_4)$
$SK = h(M' \| r_3^* \| r_4)$
$W_{new} = h(h_{Bio}(C_2 \oplus r_4))$
Replaces (W_0, W) with (W, W_{new})
$C_9 = h(SK \| r_4)$
$\{C_9\}$
$C_9 = ?h(SK \| r_4)$
Accepts SK and replaces X with

Fig. 3. Illustration of the details of our scheme.

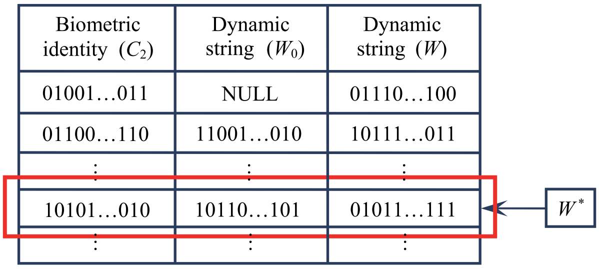
Step L1: the user U_i inputs her/his identity ID_i and password PW_i into the terminal device and then allows a scan to gain the patient user U_i's biometric information B_i. Also, the user U_i should insert her/his smart card into the terminal card reader.

Step L2: next, the user U_i chooses a random integer r_3 and uses the messages stored in the smart card to compute some valuable information $C_1^* = h(\mathrm{ID}_i||\mathrm{PW}_i||h_{\mathrm{Bio}}(B_i))$, $M^* = Y \oplus h(C_1^*)$, $r_2^* = X \oplus h(\mathrm{ID}_{\mathrm{SC}}||C_1^*||M^*)$, and $r_1^* = Z \oplus h_{\mathrm{Bio}}(T_i)$.

Step L3: for the login request message, the smart card calculates $C_3 = h_{\mathrm{Bio}}(B_i \oplus r_1^* \oplus r_2^*)$, $C_4 = B_i \oplus r_1^* \oplus h(M^*||r_3)$, and $C_5 = r_3 \oplus h_{\mathrm{Bio}}(B_i \oplus r_1^*)$ and then sends $\{C_3, C_4, C_5\}$ to the medical server S.

C. Authentication Phase

This phase should be executed after the medical server receives a login request. The user U_i and the medical server S can authenticate each other and then negotiate a common session key SK by performing the following steps.



Biometric identity (C_2)	Dynamic string (W_0)	Dynamic string (W)
01001…011	NULL	01110…100
01100…110	11001…010	10111…011
⋮	⋮	⋮
10101…010	10110…101	01011…111
⋮	⋮	⋮

Fig. 4. Our proposed dynamic verification table.

Step A1: first, the medical server S searches W^* in the dynamic verification table (shown in Fig. 4) and obtains the corresponding C_2. The medical server S first searches the column "dynamic string (W)," and if a value equals to W^*, the corresponding value in column "biometric identity" will be extracted as C_2. Otherwise, the medical server continues to search the column "dynamic string (W_0)" to see if a value equals to W^*. If successful, the medical server extracts the corresponding value C_2 and replaces W with the value of W_0. Otherwise, the medical server S rejects the user U_i's login request.

Step A2: next, the medical server S generates a random number r_4 and computes $M' = h(h_{\mathrm{Bio}}(C_2)||s)$, $r_3^* = C_5 \oplus h_{\mathrm{Bio}}(C_2)$, and $B_i \oplus r_1^* = C_4 \oplus h(M'||r_3^*)$. Then, it checks if $B_i \oplus r_1^*$ and C_2 are within a bearable threshold [20]. The session is terminated immediately if the threshold is larger than a presupposed value. On the contrary, the medical server S sends $\{C_6, C_7\}$ to the user U_i where C_6 equals to $r_4 \oplus h(B_i \oplus r_1^*)$ and C_7 equals to $h((B_i \oplus r_1^*)||r_3^*||r_4)$.

Step A3: after receiving the information $\{C_6, C_7\}$ from the medical server S, the user U_i computes $r_4^* = C_6 \oplus h(B_i \oplus r_1^*)$ and verifies whether the equation $C_7 = ?h((B_i \oplus r_1^*)||r_3||r_4^*)$ holds or not. If the verification succeeds, the user U_i computes the session key $\mathrm{SK} = h(M^*||r_3||r_4^*)$ and $X_{\mathrm{new}} = h(\mathrm{ID}_{\mathrm{SC}}||C_1^*||M^*) \oplus r_4^*$. After that, the user U_i sends $C_8 = h(h_{\mathrm{Bio}}(B_i \oplus r_1^* \oplus r_4^*) \oplus r_4^*)$ as a confirmation value to the medical server S.

Step A4: after receiving the confirmation of the user, the medical server S checks the validity of C_8 by comparing it with $h(h_{\mathrm{Bio}}(B_i \oplus r_1^* \oplus r_4) \oplus r_4)$. If these two values are the same, the medical server S accepts the session key $\mathrm{SK} = h(M'||r_3^*||r_4)$ and computes $W_{\mathrm{new}} = h(h_{\mathrm{Bio}}(C_2 \oplus r_4))$. Then, it replaces (W_0, W) with (W, W_{new}) for the user U_i's next login and sends $C_9 = h(\mathrm{SK}||r_4)$ to the user as an acknowledgment.

Step A5: after receiving C_9 from the medical server, the user checks the validity of C_9 by comparing it with $h(\mathrm{SK}||r_4)$. If these two values are the same, the user accepts the session key SK and replaces X with X_{new} in the smart card for next login. If the checking of C_9 fails or the user does not receive C_9 in a given time, the session will be terminated immediately and the user will start another session.

Finally, the user U_i and the medical server S authenticate each other and negotiate a common session key securely. Let SK_u be the session key of the user and SK_s represent the session key of the medical server. Suppose that the user and the medical server are legal. The scheme is correct if equation $\mathrm{SK}_u = \mathrm{SK}_s$ holds.

Then, we have

$$\begin{aligned}\mathrm{SK}_u &= h\left(M^* \| r_3 \| r_4^*\right)\\ &= h\left(Y \oplus C_1^* \| r_3 \| C_6 \oplus h(B_i \oplus r_1^*\right)\\ &= h\left(M \oplus C_1 \oplus C_1^* \| r_3 \| r_4 \oplus h\left(B_i \oplus r_1^*\right)\right.\\ &\quad \left.\oplus h\left(B_i \oplus {r_1}^*\right)\right)\\ &= h\left(M \| r_3 \| r_4\right)\\ &= h\left(M \| r_3 \oplus h_{\mathrm{Bio}}\left(B_i \oplus r_1^*\right) \oplus h_{\mathrm{Bio}}\left(T_i \oplus r_1^*\right) \| r_4\right)\\ &= h\left(h\left(h_{\mathrm{Bio}}\left(C_2\right) \| s\right) \| C_5 \oplus h_{\mathrm{Bio}}\left(C_2\right) \| r_4\right)\\ &= h\left(M' \| r_3^* \| r_4\right)\\ &= \mathrm{SK}_s.\end{aligned}$$

IV. Security Analysis

In this section, we show that our proposed scheme is provably secure under real-or-random model. Moreover, some other security features are discussed in Section IV-C.

A. Security Model

The security model of password-based authenticated key exchange protocol has been introduced by Bellare *et al.* [36]. We extended their model into a three-factor one by adding some new oracles in Abdalla *et al.*'s real-or-random model [37]. Those definitions are described as follows:

Participants: Let $\boldsymbol{\mathcal{U}}$ be the set of users and $\boldsymbol{S}$ be the set of servers. The set of all participants $\boldsymbol{\mathcal{P}}$ is the union of $\boldsymbol{\mathcal{U}}$ and $\boldsymbol{S}$. The symbol $\boldsymbol{u}$ represents an instance of $\boldsymbol{\mathcal{U}}$ and $\boldsymbol{s}$ denotes an instance of $\boldsymbol{S}$. Any participant instance $\boldsymbol{p}$ of set $\boldsymbol{\mathcal{P}}$ is an oracle.

Partnering: Session identifications (sid) are unique for each key agreement conversation in practice. We say that $\boldsymbol{u}$ and $\boldsymbol{s}$ are partnered if these two instances share the same non-null session identifications (sid_u).

Adversary: The adversary $\boldsymbol{A}$ in this model runs in polynomial time. The ability of the adversary $\boldsymbol{A}$ is defined by the following queries.

Execute ($\boldsymbol{u}$, $\boldsymbol{S}$): This query models the eavesdropping attacks and returns a copy of the messages transmitted between $\boldsymbol{u}$ and its partner $\boldsymbol{S}$ during their last authentication conversation.

Send ($\boldsymbol{p}$, m): The adversary sends a message *m* to $\boldsymbol{p}$ and receives a respond message in this query. It models the active attacks such as replay attacks, modification attacks, and impersonation attacks.

CorruptSC ($\boldsymbol{u}$): This query returns the current information stored in $\boldsymbol{u}$'s smart card to simulate the smart card lost attacks such as offline password guessing attacks with smart card.

CorruptDB ($\boldsymbol{s}$): The current table $\{C_2,\, W_0,\, W\}$ of s will be returned to the adversary when she/he queries the instance $\boldsymbol{s}$. The stolen verifier attack is simulated by this query.

Note that in CorruptSC and CorruptDB queries, only the current information will be delivered since the data stored in the smart card and the database change dynamically.

Test ($\boldsymbol{u}$/ $\boldsymbol{S}$): The semantic security of the session key is simulated by flipping an unbiased coin *b* in Test query. The instance $\boldsymbol{u}$ returns a random binary string if the hidden bit $b = 0$ or the session key if $b = 1$. If the adversary asks many Test queries, the output should be based on the same value of *b*.

Hash(x, h(x)): The Hash oracle searches for *x* in its table when one makes a query and returns *h*(*x*) if *x* exists; otherwise, it returns a uniformly random string *k* and stores $\{x,\, k\}$ in the table.

Biohash$(x,\, h_{\mathrm{Bio}}(x))$*:* When a query with *x* is made, the Biohash oracle compares every existing element x^* with x and returns $h_{\mathrm{Bio}}(x)$ if the number of different bits between x^* and x is within a threshold value; otherwise, a uniformly random string *k* is returned and $\{x,\, k\}$ is stored in the table.

Semantic security: Providing the above-mentioned queries, the adversary $\boldsymbol{A}$ may interact with the instances to help she/he determine the value of bit *b*. If she/he guesses correctly, the scheme fails to provide semantic security. Let Succ denote the event that $\boldsymbol{A}$ wins. $\boldsymbol{A}$ has an advantage $\mathrm{Adv}^{ake}(\boldsymbol{A}) = |2 \cdot \Pr[\mathrm{Succ}] - 1|$ in breaking the semantic security of the scheme. If $\mathrm{Adv}^{ake}(\boldsymbol{A})$ is negligible, the scheme is secure under the real-or-random model.

B. Formal Analysis in a Real-or-Random Model

Theorem 1: Let D_1, D_2, and D_3 be uniformly distributed dictionaries of user identity, password, and biometric template, respectively. $|D_1|$, $|D_2|$, and $|D_3|$ denote the size of D_1, D_2, and D_3. Then, we have

$$\begin{aligned}\mathrm{Adv}^{\mathrm{ake}} \le{}& \frac{q_h^2}{|H_1|} + \frac{q_b^2}{|H_2|}\\ &+ \max\left\{\frac{2q_s}{|D_1| \cdot |D_2| \cdot |D_3|},\, \frac{q_t}{2^{l-1} \cdot |T|}\right\}\end{aligned}$$

where q_h, q_b, and q_s denote the number of Hash queries, Biohash queries, and Send queries, respectively. $|H_1|$, $|H_2|$, and $|T|$ denote the range space of the hash function, the range space of the biohash function, and the number of the items in the server's table, respectively. q_t is the number of $\boldsymbol{A}$'s guessing attempt toward the server. As the matter of fact, $|D_3|$ is much larger than $|D_1|$ and $|D_2|$.

Proof: Let Succ_i be the event that the adversary $\boldsymbol{A}$ wins game G_i. In each game, $\boldsymbol{A}$ is supposed to guess the hidden bit b which is chosen before the starting game G_0.

Game G_0: This game models a real attack by the adversary $\boldsymbol{A}$. According to definitions mentioned above, we have

$$\mathrm{Adv}^{\mathrm{ake}}\left(\boldsymbol{A}\right) = 2 \cdot \Pr\left[\mathrm{Succ}_0\right]. \tag{1}$$

Game G_1: To increase the advantage of winning, the adversary $\boldsymbol{A}$ launches an eavesdropping attack by querying the Execute ($\boldsymbol{u},\boldsymbol{S}$) oracle. Then, $\boldsymbol{A}$ has to decide the value of b in the Test ($\boldsymbol{u}/\boldsymbol{S}$) oracle. Since the session key SK is computed by M, r_3, and r_4, $\boldsymbol{A}$ tries to extract these values from $\{C_3,\, \ldots,\, C_9\}$. According to Section III, we know that $M = Y \oplus h(\mathrm{ID}_i||\mathrm{PW}_i||h_{\mathrm{Bio}}(B_i)) = h(h_{\mathrm{Bio}}(C_2)||s)$, $r_3 = C_5 \oplus h_{\mathrm{Bio}}(C_2)$, and $r_4 = C_6 \oplus h(B_i \oplus r_1)$. Therefore, $\boldsymbol{A}$ cannot compute SK before corrupting the smart card or the server's database. The identity, the password, and the biometric template of user and server's master key remain unknown. Thus, the eavesdropping attack does not provide any advantage compared to game G_0 and we get

$$\Pr\left[\mathrm{Succ}_1\right] = \Pr\left[\mathrm{Succ}_0\right]. \tag{2}$$

Game G_2: We transfer game G_1 to this game by adding a Send query to simulate an active attack. Hash oracle and Biohash oracle also need to create fabricate messages. No collisions will be found while querying Hash oracle and Biohash oracle because every message contains some different random factors such as biometric information and random numbers. By using the birthday paradox, we have

$$\left|\Pr\left[\mathrm{Succ}_2\right] - \Pr[\mathrm{Succ}_1]\right| \leq q_h^2/2 \cdot |H_1| + q_b^2/2 \cdot |H_2|. \tag{3}$$

Game G_3: In this game, the adversary $\boldsymbol{A}$ queries the CorruptSC oracle and the CorruptDB oracle. Game G_3 is transformed from game G_2.

Case 1: the adversary $\boldsymbol{A}$ receives $\mathrm{ID}_{\mathrm{SC}}$, *X*, *Y*, and *Z* stored in the user's smart card by querying the CorruptSC oracle. Then, $\boldsymbol{A}$ tries a dictionary attack with the possible identity, password, and biometric information of the user in D_1, D_2, and D_3. Since the scale of the dictionary is $|D_1|\cdot|D_2|\cdot|D_3|$, the dictionary attacks are not available. Thus, we have

$$\left|\Pr\left[\mathrm{Succ}_3\right] - \Pr[\mathrm{Succ}_2]\right| \ \leq\ q_s/\,|D_1| \cdot |D_2| \cdot |D_3|. \tag{4}$$

Case 2: Instead of querying the CorruptSC oracle, the CorruptDB oracle is queried to simulate a stolen verification table attack. After receiving the server's table $\{C_2, W_0, W\}$, the adversary $\boldsymbol{A}$ tries every C_2 in it and starts a different online dictionary attack by calculating $M = h(h_{\mathrm{Bio}}(C_2)||s)$, $C_4^* = C_2 \oplus h(M\,||r)$, and $C_5^* = r \oplus h_{\mathrm{Bio}}(C_2)$ where *r* is a randomly chosen number. C_3^* is left for the Biohash oracle and Send $(\boldsymbol{s}, \{C_3^*, C_4^*, C_5^*\})$ is queried. $\boldsymbol{A}$ uses a random string with *l* bits to replace the server's master key *s*; so, we have

$$\left|\Pr\left[\mathrm{Succ}_3\right] - \Pr[\mathrm{Succ}_2]\right| \ \leq\ q_t/2^l \cdot |T|. \tag{5}$$

The adversary $\boldsymbol{A}$ can choose case 1 or case 2 as the last game G_3. From game G_0 to game G_3, all the oracles are simulated and $\boldsymbol{A}$ has no choice but querying the Test oracle and guessing the bit *b* in the last game. Therefore

$$\Pr\left[\mathrm{Succ}_3\right] = 1/2. \tag{6}$$

Combining (1)–(4) and (6), we have

$$\mathrm{Adv}^{\mathrm{ake}} \leq \frac{q_h^2}{|H_1|} + \frac{q_b^2}{|H_2|} + \frac{2q_s}{|D_1| \cdot |D_2| \cdot |D_3|}.$$

Combining (1)–(3) and (5) and (6), we have

$$\mathrm{Adv}^{\mathrm{ake}} \leq \frac{q_h^2}{|H_1|} + \frac{q_b^2}{|H_2|} + \frac{q_t}{2^{l-1} \cdot |T|}.$$

Thus, $\mathrm{Adv}^{\mathrm{ake}} \leq \frac{q_h^2}{|H_1|} + \frac{q_b^2}{|H_2|} + \max\{\frac{2q_s}{|D_1|\cdot|D_2|\cdot|D_3|}, \frac{q_t}{2^{l-1}\cdot|T|}\}$. The adversary does not have a non-negligible advantage since $|H_1|, |H_2|, |D_1|\cdot|D_2|\cdot|D_3|$, and $2^{l\,-1} \cdot |T|$ are beyond the polynomial time. The proposed scheme provides semantic security in our security model.

C. Discussion on Possible Attacks

In this section, we discuss the security of our proposed protocol by analyzing some possible attacks. Some possible attacks have already been analyzed by the real-or-random model in Section IV-B such as replay attacks, modification attacks, and impersonation attacks by Send oracle. We omit the analysis of these attacks and focus on some attributes we have not discussed in detail such as the resistance to man-in-the-middle attacks, perfect forward secrecy, biometric protection, etc. The following discussion shows how our proposed scheme resists the possible attacks.

Resistance to man-in-the-middle attacks: In our scheme, a session key SK is established between the user U_i and the medical server *S* only after the mutual authentication. In order to make an independent connection with the medical server *S*, the adversary $\boldsymbol{A}$ needs to deliver a legal login request message $\{C_3, C_4, C_5\}$ to pass the verification process of the medical server *S*. However, without any knowledge of C_1 *X*, *Y*, $\mathrm{ID}_{\mathrm{SC}}$, and $B_i \oplus r_1$, the adversary $\boldsymbol{A}$ cannot construct a legal C_3. If the adversary *A* cannot forge a legal C_3 called C_3', the server *S* will reject the login request for no corresponding C_2 is found using $W' = h(C_3')$. Even if the adversary *A* constructs a legal C_3, this attack can be found when the server compares the computed value of $B_i \oplus r_1^*$ and the value of C_2 from the dynamic verification table. That is because without the knowledge of U_i's biometric data B_i and the master key *s* of the server, the adversary *A* cannot generate legal C_4 and C_5 to pass the verification process of the server *S*. For the same reason, the adversary $\boldsymbol{A}$ cannot make an independent connection with the user U_i. Since the adversary $\boldsymbol{A}$ does not know the $B_i \oplus r_1^*$ and r_3, she/he is not able to generate valid C_6 and C_7 to pass the verification process of the user U_i. Thus, the adversary $\boldsymbol{A}$ cannot construct independent connections with either the medical server *S* or the user U_i. If the adversary $\boldsymbol{A}$ tries to be a man in the middle to communicate with U_i and *S* independently, U_i and *S* will detect the error and terminate the session immediately. The above-mentioned analysis shows that the proposed scheme can resist the man-in-middle attack.

Resistance to offline password guessing attacks with/without smart cards: Assuming an adversary $\boldsymbol{A}$ intercepts all the messages transmitting between the user U_i and the medical server *S*, and launches an offline dictionary attack. Since none of the transmitted messages $\{C_3, \ldots, C_9\}$ possess the user U_i's password PW_i, the adversary $\boldsymbol{A}$ cannot determine whether each of she/he guessed passwords is correct or not via the intercepted messages $\{C_3, \ldots, C_9\}$. Therefore, the adversary $\boldsymbol{A}$ cannot perform the offline dictionary attack without smart cards successfully.

Considering another case, the adversary $\boldsymbol{A}$ compromises the secret information $\{\mathrm{ID}_{\mathrm{SC}}, h(\cdot), h_{\mathrm{Bio}}(\cdot), X, Y, Z\}$ stored in the smart card of U_i and launches the offline dictionary attack with smart cards. Compared with the offline dictionary attack without smart cards, the addition information known by $\boldsymbol{A}$ in this attack is $\{\mathrm{ID}_{\mathrm{SC}}, h(\cdot), h_{\mathrm{Bio}}(\cdot), X, Y, Z\}$. In order to obtain U_i's password PW_i, the adversary needs to compromise C_1 from *X* or *Y*. Since C_1 is protected by a high entropy random integer r_2, the secret message *M*, and one way hash function, the adversary ***A*** cannot guess C_1 correctly. Furthermore, the adversary ***A*** cannot obtain C_1 from *Y* without the knowledge of $M = h(h_{\mathrm{Bio}}(C_2)||s)$ which is constructed by medical server's master key *s* and C_2. Even if the adversary ***A*** obtain $C_1 = h(\mathrm{ID}_i||\,\mathrm{PW}_i||h_{\mathrm{Bio}}(T_i))$, she/he cannot guess the user U_i's password PW_i successfully without the knowledge of U_i's biometric data T_i and identity ID_i. Thus, the offline password guessing attack with/without smart cards cannot violate our proposed scheme.

Resistance to de-synchronization attacks: In the proposed scheme, after the medical server *S* computes SK, it sends an acknowledgment message C_9 to the user. If the user receives the acknowledgment message, it stores the computed SK as the shared session key. If the message C_8 or C_9 is blocked, the user will not receive the acknowledgment message C_9 in a given time. In this case, the user will delete SK and restart the login and authentication process. And during the restart authentication phase, the medical server searches W^* in the dynamic verification table and obtains the corresponding C_2 by using the matched value W_0 (old value). So, the user and the server can negotiate a shared session key in the restart authentication process. Thus, the proposed scheme can resist desynchronization attacks.

Resistance to stolen verifier attacks: In our scheme, the verifier is the current dynamic verification table which consists $C_2 = T_i \oplus r_1$, $W = h(h_{\mathrm{Bio}}(T_i \oplus r_1 \oplus r_2))$, and W_0. W_0 could be a value of NULL or a previous *W*. Suppose that the dynamic verification table is obtained by the adversary ***A***. She/he guesses a secret key s' of the server and tries to compute $C_2' = C_4 \oplus h(h((h_{\mathrm{Bio}}(C_2)||s')||C_5 \oplus h_{\mathrm{Bio}}(C_2))$ by every C_2 in the table where C_4 and C_5 are eavesdropped by the adversary ***A***. Then, the adversary ***A*** determines whether the computed C_2' and the corresponding C_2 are within a bearable threshold. Unfortunately, she/he will fail because the master key *s* of the medical server *S* is a high-entropy random number with a length of a secure parameter *l*. The chance of guessing a correct *s* can be ignored. Thus, the stolen verifier attack will not violate the session key. Furthermore, the biometric information is still safe under this circumstance according to our analysis in paragraph "*Biometric protection*" we state below. Therefore, our scheme can resist stolen verifier attacks.

Resistance to insider attacks: On one hand, any malicious legal users will fail to impersonate other users since they have to provide the correct biometric characteristic B_i of the targeted user. On the other hand, the dynamic verification table does not consist of any information about passwords and the real biometric information in the database. The scheme remains secure even if the entire table is leaked to the adversary according to the above formal proof in the real-or-random model. Therefore, any privileged-insiders of the medical server or any malicious legal users will find the insider attack is invalid in this scheme.

Known key security: In the proposed scheme, the session key $\mathrm{SK} = h(M||r_3||r_4)$ is computed by ***M***, r_3, and r_4. r_3 and r_4 are two random integers which are generated by the user U_i and the medical server *S* respectively and independently for each session. Since r_3 and r_4 are different in each session, the session key SK in each run of the proposed scheme is unique. Therefore, the proposed scheme provides known-key security.

Perfect forward secrecy: In order to provide perfect forward secrecy, a dynamic verification table and a dynamic value stored in the smart card are designed in the proposed scheme. The adversary ***A*** can only get access to the current value rather than every previous ones. When the two private keys PW_i and *s* are leaked, ***A*** cannot compute ***M*** since $M = Y \oplus h(\mathrm{ID}_i||\mathrm{PW}_i||h_{\mathrm{Bio}}(B_i)) = h(h_{\mathrm{Bio}}(C_2)||s)$ without knowing the biometric feature B_i or verification list $\{C_2, W_0, W\}$ stored at the server. Even if the verification list is stolen, the adversary ***A*** still fails to obtain the each-round session key $\mathrm{SK} = h(M||r_3||r_4)$ because ***A*** cannot extract the related temporary information r_3 and r_4. Therefore, the proposed scheme provides perfect forward secrecy.

Biometric protection: In this scheme, attempts have been made to guarantee that the biometric feature B_i is possessed by only one entity, namely, the user itself, which results in that the only way to acquire B_i is by scanning the user's fingerprint or iris. The related values in the storage are $Z = r_1 \oplus h_{\mathrm{Bio}}(T_i)$ in the smart card and $C_2 = T_i \oplus r_1$ in the database on the medical server. The random number r_1 cannot be known unless someone provides the right biometric characteristic and one of the related values *Z* or C_2 is lost simultaneously. And the biometric template T_i cannot be retrieved by the related values *Z* or C_2 unless someone correctly guesses the random number r_1. Thus, the proposed scheme protects the privacy of the biometric successfully.

User anonymity including the untraceability: Biological feature differs from person to person. In the proposed scheme, the biometric information acts as the identifier and provides higher anonymity since a jitter exists in the scan result of biometric features. Furthermore, a new random number r_4 is generated by the medical server after every successful login. In the next login phase, C_3 equals $h_{\mathrm{Bio}}(B_i \oplus r_1 \oplus r_4)$ and *W* equals $h_{\mathrm{Bio}}(C_2 \oplus r_4)$. The random number r_3 in C_4 and C_5 and the random number r_4 in C_6, C_7 and C_8 are generated again. Thus, the linkage in the messages depends on the randomness of the random numbers. Therefore, our proposed scheme achieves the user untraceability and the user anonymity can then be provided.

V. Performance Comparison

In this section, we evaluate the performance of our proposed scheme with other four related schemes [8], [19], [21], [23] based on three-factor authentication. The computational cost and the communication cost in the login phase and the authentication phase are compared in detail and the security features of these schemes are also analyzed.

In the proposed scheme, the traditional verification table is improved to form a dynamic one which can resist the stolen verifier attack and the insider attack. And the biometric characteristics are authenticated at the server side, which forbids the online dictionary attack. In addition, the value stored in the smart card cannot be used for the offline dictionary attack since they are combined with high-entropy integers. Even if the smart

TABLE II
COMPARISON OF SECURITY FEATURES BETWEEN OUR SCHEME AND OTHERS

	[21]	[23]	[8]	[19]	Ours
Resistance to replay attacks	Y	Y	N	Y	Y
Resistance to impersonation attacks	N	Y	Y	Y	Y
Resistance to man-in-the-middle attacks	N	Y	Y	Y	Y
Resistance to modification attacks	Y	Y	Y	Y	Y
Resistance to password guessing attacks	–	Y	Y	Y	Y
Resistance to smart card lost attacks	–	Y	Y	N	Y
Resistance to online/offline dictionary attacks	–	Y	Y	N	Y
Resistance to stolen verifier attacks	Y	Y	Y	Y	Y
Resistance to insider attacks	Y	N	Y	Y	Y
Resistance to de-synchronization attacks	N	Y	N	N	Y
Perfect forward secrecy	N	Y	N	Y	Y
Mutual authentication	N	Y	Y	Y	Y
Session key security	–	Y	Y	Y	Y
User anonymity & untraceability	–	Y	N	Y	Y
Biometric protection	Y	N	N	N	Y
Formal security analysis/proof	N	Y	Y	N	Y

TABLE III
COMPARISON OF COMPUTATIONAL COST

	Hash & Biohash operations	Other operations	Total execute time (ms)
Yeh *et al.* [21]	$3T_h$	$4T_m + 12T_a$	3.4508
Wu *et al.* [23]	$12T_h + 1T_{\mathrm{bh}}$	$4T_m + 4T_s$	3.2252
Amin *et al.* [8]	$10T_h + 1T_{\mathrm{bh}}$	–	0.0819
Li *et al.* [19]	$10T_h + 1T_{\mathrm{bh}}$	$4T_e$	6.6610
Ours	$19T_h + 4T_{\mathrm{bh}}$	–	0.0989

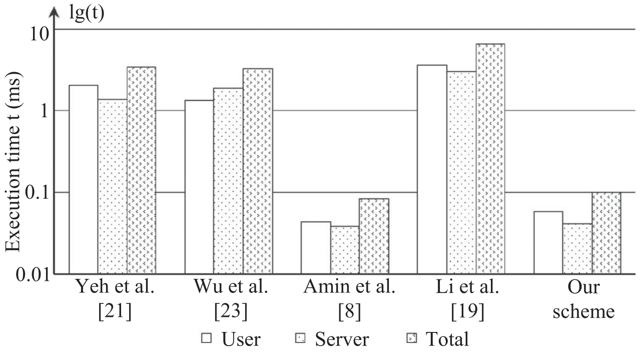


Fig. 5. Execution time comparisons between our scheme and others.

card is lost, no user information will be leaked out. As for the transmitting messages, the linkage between any two messages is broken by the implementation of high-entropy integers and the biometric information's jitter. Thus, anonymity and untraceability have been achieved.

As shown in Table II, the related schemes [8], [19], [21], [23] have some design flaws and cannot satisfy all the security features. Yeh *et al.*'s scheme [21] focuses on preventing the insider attack, but suffers from the impersonation attack and fails to establish a secure session key. Wu *et al.*'s scheme [23] satisfies most of the security requirements, whereas they ignore the insider attack. Amin *et al.*'s scheme [8] cannot provide several security features since the replay attack is not prevented and the perfect forward secrecy is not satisfied. In Li *et al.*'s scheme [19], the smart card stores a value $V = h(\mathrm{ID}||h(\mathrm{PW}||h_{\mathrm{Bio}}(\mathrm{BD}))$ which could cause the offline smart card breach attacks and other problems. Furthermore, the schemes [8], [19], [21] suffered from desynchronization attacks. Compared with the related works [8], [19], [21], [23], our proposed scheme can resist most of the known attacks and provides a number of attractive security features especially privacy protection.

The computational cost of our proposed scheme is also compared with other related schemes. We carried out a simulation of these schemes with OpenSSL Library on two different computers. The hardware platform for the user is Inter(R) Pentium(R) CPU G630 which offers maximum clock speeds of 2.70 GHz and 4.00 GB memory. The server is given an Inter(R) Core(TM) i5-3337 U CPU @ 1.80 GHz and 4.00 GB memory. Those two PCs were connected with a switch to simulate a practical environment. The switch we adopted is H3C S1024R which ensures the bandwidth between any two connected network devices is 100 Mbps. Each of the simulation was performed for 100 times and the average results are shown in Table III. The notation T_h and T_{bh} denote the time for executing a one-way hash or biohash function, respectively. And let T_s, T_m, T_a, and T_e be the time for executing a symmetric key encryption/decryption operation, the time for executing a scalar multiplication operation of an elliptic curve, the time for executing a point addition operation of an elliptic curve, and the time for executing a modular exponentiation operation, respectively. The hash function we adopted is an SHA-1 algorithm. And the biohash algorithm we used in our simulation is based on [38]. The length of the biometrics we used in our simulation is 160 bits. During the simulation of Wu *et al.*'s scheme [23], we consider that the user's private key is generated in the registration phase; otherwise, the result would be incredibly large. Table III shows computational comparisons between the proposed scheme and other related schemes in the login and authentication phases. Note that the registration phase just needs to be executed only once for a certain user. The login phase and the authentication phase should be performed every time when a certain user needs medical service. As shown in Table III, compared with other related schemes [19], [21], [23], our proposed scheme and Amin *et al.*'s scheme [8] have a great advantage on computational costs, which are 0.0989 and 0.0819 ms, respectively. That is because only hash and biohash operations are adopted in our scheme and Amin *et al.*'s scheme.

As shown in Fig. 5, the computational costs in schemes [19], [21], [23] are much higher than our proposed scheme and Amin *et al.*'s scheme [8]. The reason can be concluded from Table III that those schemes involve heavyweight operations such as modular exponentiation operations and scalar multiplication operations of an elliptic curve. Thus, they are not suitable for e-health systems due to the limited computational capability of the devices. Compared with Amin *et al.*'s scheme [8], the computational overhead of our scheme costs a little more to offer more security features such as perfect forward secrecy, mutual

TABLE IV
COMPARISON OF COMMUNICATION COST

	Yeh *et al.* [21]	Wu *et al.* [23]	Amin *et al.* [8]	Li *et al.* [19]	Our scheme
Length (bytes)	448	200	132	144	164

authentication, the user anonymity, and the user untraceability which are not provided by Amin *et al.*'s scheme.

The comparison of communication cost is shown in Table IV. In our experiments, the timestamp is 4 bytes (32 bits), the output of the hash function is 20 bytes (160 bits), the output of the biohash function and modular exponentiation operation are 32 bytes (256 bits), and a point of elliptic curve is 64 bytes (512 bits). In addition, the output of a 256 bit AES is based on the input of the plaintext. Yeh *et al.*'s scheme [21] takes the largest communication load which needs 448 bytes while Amin *et al.*'s scheme [8] takes the smallest load which is 132 bytes. Wu *et al.*'s scheme [23] and Li *et al.*'s scheme [19] need 200 and 144 bytes, respectively. Our proposed scheme costs 164 bytes, which is 32 bytes more than the smallest, but it does not cause a large burden to the network obviously. Besides, the proposed scheme can resist various attacks and provide more security features. The performance on computational cost is also promising since only lightweight operations are used in the proposed scheme. Therefore, our proposed scheme is a successful authenticated key agreement protocol for e-health systems.

VI. Conclusion

In this paper, we proposed a three-factor authenticated key agreement scheme for e-health systems to protect the user's privacy using a dynamic authentication mechanism. The introduction of performing the biometric authentication at the server side complemented the weaknesses in two-factor schemes. The traditional identity-password table was replaced by a dynamic verification table to provide untraceability thus the user anonymity can be fully preserved. In addition, our scheme only adopted lightweight hash and biohash operations, which reduced the computational cost and communication cost in comparison with other related works. We also proved the proposed scheme to be semantic secure under the real-or-random model. Therefore, the proposed scheme can meet the energy consumption demands and security needs of e-health systems successfully.

References

[1] J. Kim, "Energy-efficient dynamic packet downloading for medical IoT platforms," *IEEE Trans. Ind. Informat.*, vol. 11, no. 6, pp. 1653–1659, Dec. 2015.

[2] D. B. He and S. Zeadally, "Authentication protocol for an ambient assisted living system," *IEEE Commun. Mag.*, vol. 53, no. 1, pp. 71–77, Jan. 2015.

[3] E. J. Yoon and K. Y. Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem," *J. Supercomput.*, vol. 63, pp. 235–255, Jan. 2013.

[4] M. S. Farash and M. A. Attari, "Cryptanalysis and improvement of a chaotic map-based key agreement protocol using Chebyshev sequence membership testing," *Nonlinear Dyn.*, vol. 76, pp. 1203–1213, Apr. 2014.

[5] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 35, pp. 1646–1656, Sep. 2012.

[6] X. X. Li, W. D. Qiu, D. Zheng, K. F. Chen, and J. H. Li, "Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards," *IEEE Trans. Ind. Electron.*, vol. 57, no. 2, pp. 793–800, Feb. 2010.

[7] J. L. Tsai, N. W. Lo, and T. C. Wu, "Novel anonymous authentication scheme using smart cards," *IEEE Trans. Ind. Informat.*, vol. 9, no. 4, pp. 2004–2013, Nov. 2013.

[8] R. Amin, S. K. H. Islam, G. P. Biswas, M. K. Khan, and X. Li, "Cryptanalysis and enhancement of anonymity preserving remote user mutual authentication and session key agreement scheme for E-Health care systems," *J. Med. Syst.*, vol. 39, Nov. 2015, Art. no. 140.

[9] 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, pp. 1–15, Sep. 2014.

[10] S. K. H. Islam, "Provably secure dynamic identity-based three-factor password authentication scheme using extended chaotic maps," *Nonlinear Dyn.*, vol. 78, pp. 2261–2276, Nov. 2014.

[11] T. F. Vallent and H. Kim, "Three factor authentication protocol based on bilinear pairing," in *Multimedia and Ubiquitous Engineering: MUE 2013*, J. J. Park, J. K.-Y. Ng, H.-Y. Jeong, and B. Waluyo, Eds. Dordrecht, The Netherlands: Springer, 2013, pp. 253–259.

[12] C. T. Li and M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *J. Netw. Comput. Appl.*, vol. 33, pp. 1–5, Jan. 2010.

[13] X. Li, J. W. Niu, J. Ma, W. D. Wang, and C. L. Liu, "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards," *J. Netw. Comput. Appl.*, vol. 34, pp. 73–79, Jan. 2011.

[14] A. K. Das, "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards," *IET Inf. Secur.*, vol. 5, pp. 145–151, 2011.

[15] Y. An, "Security analysis and enhancements of an effective biometric-based remote user authentication scheme using smart cards," *J. Biomed. Biotechnol.*, vol. 2012, 2012, Art. no. 519723.

[16] M. K. Khan and S. Kumari, "An improved biometrics-based remote user authentication scheme with user anonymity," *BioMed Res. Int.*, vol. 2013, 2013, Art. no. 491289.

[17] C.-I. Fan and Y.-H. Lin, "Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics," *IEEE Trans. Inf. Forensics Secur.*, vol. 4, no. 4, pp. 933–945, Dec. 2009.

[18] X. L. Li, Q. Y. Wen, W. M. Li, H. Zhang, and Z. P. Jin, "Secure privacy-preserving biometric authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 38, Nov. 2014, Art. no. 139.

[19] X. L. Li, Q. Y. Wen, and W. M. Li, "A three-factor based remote user authentication scheme: Strengthening systematic security and personal privacy for wireless communications," *Wireless Pers. Commun.*, vol. 86, pp. 1593–1610, Feb. 2016.

[20] L. Zhang, S. Zhu, and S. Tang, "Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme," *IEEE J. Biomed. Health Inf.*, vol. 21, no. 2, pp. 465–475, Mar. 2017.

[21] H. L. Yeh, T. H. Chen, K. J. Hu, and W. K. Shih, "Robust elliptic curve cryptography-based three factor user authentication providing privacy of biometric data," *IET Inf. Secur.*, vol. 7, pp. 247–252, Sep. 2013.

[22] L. L. Xu and F. Wu, "Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care," *J. Med. Syst.*, vol. 39, Feb. 2015, Art. no. 10.

[23] F. Wu, L. L. Xu, S. Kumari, and X. Li, "A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client-server networks," *Comput. Elect. Eng.*, vol. 45, pp. 274–285, Jul. 2015.

[24] Q. Jiang, M. K. Khan, X. Lu, J. F. Ma, and D. B. He, "A privacy preserving three-factor authentication protocol for e-Health clouds," *J. Supercomput.*, vol. 72, pp. 3826–3849, Oct. 2016.

[25] O. Mir and M. Nikooghadam, "A secure biometrics based authentication with key agreement scheme in telemedicine networks for E-health services," *Wireless Pers. Commun.*, vol. 83, pp. 2439–2461, Aug. 2015.

[26] J. Srinivas, S. Mukhopadhyay, and D. Mishra, "Secure and efficient user authentication scheme for multi-gateway wireless sensor networks," *Ad Hoc Netw.*, vol. 54, pp. 147–169, Jan. 2017.

[27] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, vol. 38, pp. 97–139, 2008.

[28] A. B. J. Teoh, Y. W. Kuan, and S. Lee, "Cancellable biometrics and annotations on BioHash," *Pattern Recognit.*, vol. 41, pp. 2034–2044, Jun. 2008.

[29] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Trans. Comput.*, vol. 55, no. 9, pp. 1081–1088, Sep. 2006.

[30] E. J. C. Kelkboom, J. Breebaart, I. Buhan, and R. N. J. Veldhuis, "Maximum key size and classification performance of fuzzy commitment for Gaussian modeled biometric sources," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 4, pp. 1225–1241, Aug. 2012.

[31] H. Kang, Y. Hori, T. Katashita, M. Hagiwara, and K. Iwamura, "Cryptographic key generation from PUF data using efficient fuzzy extractors," in *Proc. 16th Int. Conf. Adv. Commun. Technol.*, New York, NY, USA, 2014, pp. 23–26.

[32] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," *IEEE Trans. Inf. Forensics Secur.*, vol. 2, no. 4, pp. 744–757, Dec. 2007.

[33] Z. Jin, A. B. J. Teoh, B. M. Gor, and Y. H. Tay, "Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation," *Pattern Recognit.*, vol. 56, pp. 50–62, Aug. 2016.

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

[35] J. S. Yu, G. L. Wang, Y. Mu, and W. Gao, "An efficient generic framework for three-factor authentication with provably secure instantiation," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 12, pp. 2302–2313, Dec. 2014.

[36] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in *Advances in Cryptology - Eurocrypt 2000*, vol. 1807, B. Preneel, Ed. Berlin, Germany: Springer-Verlag, 2000, pp. 139–155.

[37] M. Abdalla, P. A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Public Key Cryptography - Pkc 2005*, vol. 3386, S. Vaudenay, Ed. Berlin, Germany: Springer-Verlag, 2005, pp. 65–84.

[38] A. Lumini and L. Nanni, "An improved BioHashing for human authentication," *Pattern Recognit.*, vol. 40, pp. 1057–1065, Mar. 2007.

Liping Zhang received the Ph.D. degree in information security from Huazhong University of Science and Technology, Wuhan, China, in 2009.

She is an Associate Professor of information security with China University of Geosciences, Wuhan, China. She has published more than 30 research papers, most of which are refereed international journal papers including IEEE/ACM/IET journal papers. Her research interests include key management and distribution, VoIP communications security, and network security. She is the principal grant holder of three externally funded research projects.

Yixin Zhang received the B.Sc. degree in information security in 2016 from China University of Geosciences, Wuhan, China, where she is currently working toward the Postgraduate degree in information security.

Her research interests include communications security, body area networks, and network security.

Shanyu Tang (A'08–M'08–SM'10) received the Ph.D. degree in computerized instrumentation from Imperial College London, London, U.K., in 1995.

He is a Professor of information security with the University of West London (UWL), London, U.K., where he leads the Cyber Security Research Group. Prior to joining UWL in 2017, he was a Distinguished Professor of information security and the Director of the Secure Communication Institute, China University of Geosciences (CUG). He joined CUG in 2012 from London Metropolitan University, where he had been a Senior Lecturer in informatics and multimedia since 2002, having joined academia in 2000 as a Lecturer in informatics and multimedia technology at the University of North London, London, U.K. He has contributed to 98 scientific publications—59 refereed journal papers including IEEE/ACM Transactions and IEE/IET journal papers, 37 conference papers, and two books. His major research interests include covert communications, multimedia security, and digital steganography.

Prof. Tang has received seven externally funded research grants, including three grants from the British Government, since 2007, as a PI and a lead academic.

He Luo received the B.Sc. degree in information security in 2015 from China University of Geosciences, Wuhan, China, where he is currently working toward the Postgraduate degree in information security.

His research interests include communications security, sensor networks, and network security.