Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme

Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme

L.P. Zhang, S.H. Zhu, S. Tang*, *Senior Member, IEEE*

***Abstract*—Telecare Medicine Information Systems (TMIS) provides flexible and convenient e-health care. However the medical records transmitted in TMIS are exposed to unsecured public networks, so TMIS are more vulnerable to various types of security threats and attacks. To provide privacy protection for TMIS, a secure and efficient authenticated key agreement scheme is urgently needed to protect the sensitive medical data. Recently, Mishra et al. proposed a biometrics-based authenticated key agreement scheme for TMIS by using hash function and nonce, they claimed that their scheme could eliminate the security weaknesses of Yan et al.'s scheme and provide dynamic identity protection and user anonymity. In this paper, however, we demonstrate that Mishra et al.'s scheme suffers from replay attacks, man-in-the-middle attacks and fails to provide perfect forward secrecy. To overcome the weaknesses of Mishra et al.'s scheme, we then propose a three-factor authenticated key agreement scheme to enable the patient enjoy the remote**

S. Tang is with the School of Computer Science at China University of Geosciences, Wuhan 430074, China. phone: +86 (27) 6784 8563; fax: +86 (27) 6784 8563; e-mail: shanyu.tang@ gmail.com

healthcare services via TMIS with privacy protection. The chaotic map-based cryptography is employed in the proposed scheme to achieve a delicate balance of security and performance. Security analysis demonstrates that the proposed scheme resists various attacks and provides several attractive security properties. Performance evaluation shows that the proposed scheme increases efficiency in comparison with other related schemes.

***Index Terms*—Telecare medicine information systems; Privacy protection; Authenticated key agreement; Chaotic maps; Security**

I. INTRODUCTION

A dvances in information technology and environmental concerns boost the rapid development of Electronic Medical Record/Electronic Health Record (EHR) systems, which collect, store, manage and share patient's healthcare associated information. Compared with traditional paper-based method, EMR/EHR provides low cost, high quality and more flexible medical records [1]. Owing to this transmission, Telecare Medicine Information Systems (TMIS) have been deployed to provide healthcare delivery services by accessing EMR/EHR via the public network like Internet [2]. In a typical medical application scenario of TMIS as shown in Fig. 1, patients submit their healthcare data to a telecare server via wired/wireless medical devices in their home. After receiving the patient's medical records, the doctors perform the diagnosis at their clinical center and then transform the final clinical decisions and treatments to the patients through the Internet. Since the TMIS realizes convenient and efficient healthcare beyond the limitation of geographical distance, it attracts great attention and spreads into the market quickly [3-6].

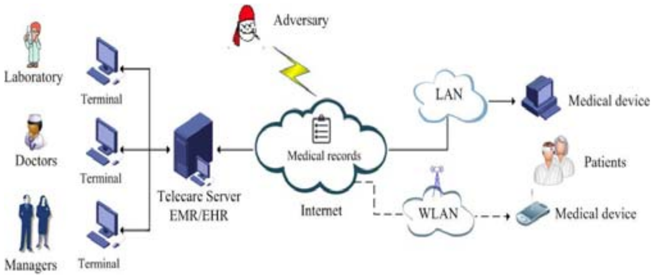

Fig. 1 Typical medical application scenario of TMIS.

However, the sensitive medical records transmitted over the the Internet are not protected in most TMIS environments, and various attacks could be launched successfully by malicious adversaries. To protect patient's medical records, TMIS based healthcare should satisfy fundamental security and privacy requirements such as authentication, confidentiality, integrity, and user anonymity [7, 8]. As the authentication mechanism can prevent the medical resources from being accessed by malicious attackers and the session key used to encrypt the packets can ensure the confidentiality of EMR/HER, many authenticated key agreement schemes [9-13] have been developed to protect medical records security and preserve patient's privacy. For example, the authentication schemes for HIPAA privacy and security regulations [9-11] were proposed to provide authorization, authentication and key management. The software solution [12] for sharing and querying of HL7 version 3 clinical documents was presented to provide security for data providers and protect the patients' privacy.

Recently, passwords and smartcards based authenticated key agreement schemes have been studied widely for TMIS [14-19]. However, these schemes have some limitations. Firstly, both smartcards and passwords could be forgotten, lost, stolen or duplicated. Secondly, if the authorized users share their smart cards and passwords with unauthorized users, there is no way for the system to tell who the actual user is. Thirdly, some of these schemes [14-15] require the server to maintain a password table for verification purposes, making them suffers from some possible attacks such as password disclosure attacks, stolen-verifier attacks and server-spoofing attacks. Besides, user's passwords are potentially vulnerable to offline password guessing attacks since their entropy are usually very low. To enhance the security, biometric characteristics are employed as a third factor to design a strong authentication scheme. Since the combination of the three factors can resist guess, forget, stolen, and duplicate issues [20], the three factors-based authentication schemes overcome the weaknesses existing in two-factor schemes. As the three factors provide many attractive properties, several three-factor authentication and key agreement schemes have been proposed for TMIS [21-28].

In order to design a three-factor authenticated key agreement scheme, several cryptographic algorithms were employed such as one-way hash function, Chaotic maps, Elliptic Curve Cryptography (ECC), RSA cryptosystem and some other operations like X-OR and concatenate etc. Compared with RSA, ECC offers equivalent security with smaller key sizes which implies lower power, bandwidth, and computational requirements [29-31]. In addition, the computation of chaotic map operations is less complex than the ECC and RSA [32-36], so it is more efficient for designing a mutual authentication scheme.

By deploying symmetric key encryption technique and hash function, Awasthi and Srivatava [21] proposed a lightweight three-factor authenticated key agreement scheme for TMIS. Although their design is efficient, several security drawbacks were identified by Mishra et al. [22] and Tan [23]. Mishra et al. pointed out that Awasthi and Srivatava's scheme could not resist password guessing attacks. Besides, their scheme failed to detect the wrong input in password change phase, and this failure might cause denial-of-service attacks in future login phase. Tan demonstrated that Awasthi and Srivatava's scheme was vulnerable to reflection attacks and did not achieve user anonymity and three-factor security. To tackle these problems, Tan presented an improved scheme. However, later analysis [24] showed that Tan's scheme suffered from replay attacks and denial-of-service attacks. To overcome the weaknesses, Yan et al. [25] proposed a new scheme and claimed that their scheme was secure against various attacks. Nevertheless, Mishra et al. [26] argued that Yan et al.'s design was vulnerable to offline password guessing attacks, and failed to provide efficient login and password updating as well as user anonymity. And then, they presented an authentication scheme by using the hash function and nonce to enhance the security. Recently, Mrudula et al.'s [27] pointed out that Mishra et al.'s scheme [26] was insecure against the offline identity guessing attack and the user impersonation attack. Amin and Biswas [28] argued that Mishra et al.'s scheme [26] could not withstand the server impersonation attack, the session key computation attack and the smart card theft attack. In this paper, we demonstrated that Mishra et al. scheme [26] could not resist the replay attack and the man-in-the-middle attack, and failed to provide perfect forward secrecy.

To enhance the security while still preserve the efficiency of Mishra et al.'s scheme [26], in this study, we develop an improved authenticated key agreement scheme for TMIS which enables the patients to enjoy the remote healthcare services securely and anonymously. Although Amin et al. [28] presented an improvement scheme based on Mishra et al.'s scheme, their scheme suffered from the known session specific temporary information attack [37] and increase the computational costs. In order to achieve a delicate balance between performance and security, chaotic map-based cryptography [38] is employed in the proposed scheme. Since chaotic map operations possess the semi-group property, it is more efficient than modular exponential computation and point multiplication operations of elliptic curve [32-36, 39-40]. The proposed three factor authentication scheme not only achieves mutual authentication and key agreement by using Chebyshev chaotic map but also enhances the performance in comparison with other related schemes.

The rest of this paper is organized as follows. Section II briefly review Mishra et al.'s scheme [26]. Section III describes a cryptanalysis of Mishra et al.'s scheme [26]. Our authenticated key agreement scheme is presented in Section IV. In Section V, the security of the proposed scheme is discussed. The performance of the scheme is examined in Section VI, and the paper is concluded in Section VII.

II. REVIEW OF MISHRA ET AL.'S SCHEME

In this section, we briefly review Mishra et al.'s biometrics based authentication scheme [26]. Their protocol consists of five phases: registration phase, login phase, authentication phase, and password and biometrics update phase. The notations used throughout this paper are summarized in TABLE I.

TABLE I

Notations and Terminology

Symbol	Notations and terminology
S	Telecare server in TMIS
U_i	Patients in TMIS

SC	Smart card
ID_i	The identity of the patient U_i
PW_i	The password of the patient U_i
B_i	The biometric data of the patient U_i
mk	The master key of the telecare server S
$h(.)$	Secure one-way hash function
$H(.)$	Secure Biohashing function
$E_k(.)$	Symmetric key encryption algorithm using k
$D_k(.)$	Symmetric key decryption algorithm using k
$T_u(x)$	Chebyshev chaotic map operation
Δ	Matching algorithm of biometrics
$\|\|$	String concatenation operation
$\oplus$	Exclusive-or operation

A. Registration phase

When a patient U_i wants to register in the TMIS, it performs following steps with the telecare server S through a secure channel.

*Step R*1: the patient U_i selects its identity ID_i, its password PW_i and a random number N_i. Then it imprints its biometrics B_i via the sensor and computes $W = h(ID_i \| PW_i \| N_i)$. Finally, U_i submits (W, ID_i) to the telecare server S.

*Step R*2: the telecare server *S* chooses a high entropy integer *x* as its private key. And then it computes $X_i = h(ID_i \| x)$, $Y_i = X_i \oplus W$, and generates *U*U_i's dynamic identity $NID = E_x(\ ID_i \| R)$, where *R* is a random integer. Next, *S* stores {*NID*, Y_i, *h*(.)} into the smart card and submits it to U_i .

*Step R*3: upon receiving the smart card, U_i computes *N*= $N_i \oplus H(B_i)$ and $V_i = h(ID_i \| PW_i \| N_i)$. Next it stores (*N*, V_i) into the smart card and keep the smart card secretly.

B. Login phase

When a patient U_i accesses to the telecare server, it inserts its smart card into the card reader. And then the smart card and the telecare server execute the following steps:

*Step L*1: the patient U_i inputs (ID_i, PW_i) and imprints its biometrics B_i via a sensor.

*Step L*2: the smart card computes $N = N_i \oplus H(B_i)$ and verifies whether the equation $V_i = h(ID_i \| PW_i \| N_i)$ holds. If it is invalid, the login session is rejected. Otherwise, the smart card computes $W = h(ID_i \| PW_i \| N_i)$, $X_i = Y_i \oplus W$ and generates r_i to obtain $a_i = h(ID_i \| X_i \| r_i)$. At last, the smart card sends login message {*NID*, a_i, r_i} to the telecare server *S*.

C. Authentication phase

Upon receiving the login message, the telecare server *S* and the patient U_i perform the following steps to achieve mutual authentication.

*Step A*1: the telecare server *S* retrieves ID_i by decrypting *NID* from the receiving message. Then it computes $X_i = h(ID_i \| x)$ and verifies whether the equation $a_i = h(ID_i \ \| X_i \| r_i)$ holds. If the verification does not hold, *S* terminates the session. Otherwise, *S* generates two random integers r_s and R' to compute the shared session key $sk = h(ID_i \| X_i \| r_i \| r_s)$, $NID' = E_x(ID_i \| R')$ and $b_i = h(ID_i \| NID \| sk \| NID')$. Afterwards, *S* sends $\{r_s, b_i, h(sk \| ID_i) \oplus NID')$ to the patient U_i.

*Step A*2: after receiving the message, the smart card computes the shared session key $sk = h(ID_i \| X_i \| r_i \| r_s)$ and retrieves the U_i's dynamic identity $NID' = h(sk \| ID_i) \oplus h(sk \| ID_i) \oplus NID'$. Then, it verifies whether the result of $h(ID_i \| NID \| sk \| NID')$ is equal to the received message b_i. If not, the smart card stops the session. Otherwise, the smart card computes $c_i = h(ID_i \| NID' \| sk)$ and sends c_i as the session key verification message to the telecare server S.

*Step A*3: upon receiving the message c_i, the telecare server S verifies whether the equation $c_i = h(ID_i \| NID' \| sk)$ holds. If not, it terminates the authentication session. Otherwise, U_i is authenticated, and the shared session key sk is valid.

D. Password and biometrics update phase

The patient can change its password and biometric without server assistance.

*Step P*1: the patient U_i inserts the smart card into the card reader and inputs its identity ID_i and its password PW_i, and then imprints its biometrics B_i via a sensor.

*Step P*2: the smart card checks whether all the inputs are valid. If not, it stops the session. Otherwise, the smart card requires the patient to submit her/his new identity information.

*Step P*3: the patient U_i selects a new password PW_i', a new random number N_i', and imprints a new biometrics B_i'.

*Step P*4: upon receiving the message, the smart card computes $W = h(ID_i \| PW_i \| N_i)$, $W_{new} = h(ID_i \| PW_i' \| N_i')$, $Y_{new} = Y_i \oplus W \oplus W_{new}$, $V_{new} = h(ID_i \| PW_i' \| N_i')$ and $N_{new} = N \oplus H(B_i')$. Finally, the smart card replaces the old message (Y_i, N_i, V_i) with the new identity information (Y_{new}, N_{new}, V_{new}).

III. CRYPTANALYSIS OF MISHRA ET AL.'S SCHEME

In this section, we describe our findings that the scheme of Mishra et al. [26] is vulnerable to the replay attack, the man-in-the-middle attack, and failed to provide perfect forward. Before that, an attacker model [41, 42] is defined as follows.

A. Attack model

1)The adversary can extract the values stored in the smartcard by some ways like monitoring their power consumption and reverse engineering techniques [43, 44].

2)The adversary can control the communication channel, that is, it may eavesdrop, intercept, modify, remove, and replay any message transmitted over the public channel.

3)The adversary may be a legitimate but malicious user or server in TMIS.

4) An attacker can guess a low entropy password and identity individually easily but guessing two secret parameters (e.g. password, identity) is computationally infeasible in polynomial time [45].

Under these assumptions, an attacker Eve can extract the information $\{NID, Y_i, N, V_i\}$ from the smartcard, and record all the messages transmitted via the public channel. Then, the scheme cannot resist the offline identity guessing attack, the replay attack, the Man-in-the-middle attack and fails to provide perfect forward secrecy.

B. Suffer from the offline identity guessing attack

In this subsection, we review that Mishra et al.'s scheme suffers from offline identity guessing attacks which demonstrated by Mrudula et al. [27]. And we also discuss why this attack can be easily launched.

Assume that the adversary *Eve* compromises the secret information（NID, Y_i, N, V_i）stored in the smart card and eavesdrops previous login messages（NID, a_i, r_i）. In Mishra et al.'s scheme [26], since the secret information $V_i = h(ID_i \| PW_i \| N_i) = W$, *Eve* can deduce that $a_i = h(ID_i \| X_i \| r_i) = h(ID_i \| Y_i \oplus W \| r_i) = h(ID_i \| Y_i \oplus V_i \| r_i)$. Then, she can launch the offline identity guessing attack to obtain the patient real identity. First, *Eve* guesses the value of ID_i^* from an identity dictionary space and then computes $a_i^* = h(ID_i^* \| Y_i \oplus V_i \| r_i)$ where Y_i and V_i are stored in the smart card and r_i is eavesdropped from the public channel. Then, *Eve* compares the computed value a_i^* with the intercepted value a_i. If they are equal, *Eve* gets the correct identity of the patient U_i. Otherwise, *Eve* selects another identity from the dictionary and try it again until finds the correct identity. Once the adversary successfully guesses the patient's identity, she/he can trace and derive valuable messages of the patient. Therefore, Mishra et al.'s scheme [26] cannot achieve user anonymity and user untraceability.

Since the identity guesses attack mentioned above do not need to interact with the telecare server, this attack is easy to launch. Suppose that the length of patient U_i's identity space is $|\pi_i|$ and the time complexity of this attack process is $O(|\pi_i| \cdot T_h)$, here T_h denotes the time for operating a hash function. Since the function $O(|\pi_i| \cdot T_h)$ is a linear function of U_i's identity space, the identity guesses attack mentioned above is a lightweight attack.

C. Suffer from the replay attack

From above analysis, the attacker can obtain the valid identity by launching the offline identity guessing attack. Then, we demonstrate Mishra et al.'s scheme [26] suffers from replay attack using the compromised identity. Suppose an adversary *Eve* records the old login message and replays it to the telecare server *S*. Then *Eve* can retrieve the new dynamic identity NID' from the receiving message $\langle r_s^*, b_i, h(sk \| ID_i) \oplus NID' \rangle$ by using the computed session key $sk^* = h\left(ID_i \| Y_i \oplus V_i \| r_i \| r_s^*\right)$ via the compromised identity *ID*$_i$ and the message (*Y*$_i$, *V*$_i$) stored in the smart card. Consequently, *Eve* can construct a valid $c_i = h\left(ID_i \| NID' \| sk^*\right)$ to pass the verification of telecare server *S*. Under this case, the adversary *Eve* could be authenticated as a legal patient by launching the replay attacks.

D. Suffer from the Man-in-the-middle attack

Since the adversary Eve can impersonate a patient *U*$_i$ to cheat the telecare server *S* [27], then she can share a session key with the telecare server *S* and makes it believes that the key is shared with the patient *U*$_i$. On the other hand, Eve can also impersonate the telecare server *S* [28], so that she can convince the patient *U*$_i$ to share a session key, making it believes that the key is shared with the telecare server *S*. Therefore, Mishra et al.'s scheme [26] could not resist the man-in-the-middle attack.

E. No provision of perfect forward secrecy

In Mishra et al.'s scheme [26], once the telecare server's long-term private key *x* is revealed, all the previous session keys would be compromised. Suppose that an adversary Eve has compromised the secret private key *x* and obtained previous messages. Then the adversary *Eve* intercepts the login messages {*NID*, *a*$_i$, *r*$_i$} and obtains the patient *U*$_i$'s real identity by decrypting $NID = E_x(ID_i \| R)$ with the compromised private key *x*. Next, *Eve* can compute $X_i = h(ID_i \| x)$ via the compromised identity *ID*$_i$, and then she can computes the previous session keys $sk = h(ID_i \| X_i \| r_i \| r_s)$ by using the computed *X*$_i$, the compromised identity *ID*$_i$ and the intercepted message (*r*$_i$, *r*$_s$).

Since the security of Mishra et al.'s scheme [26] is independent on some intractable mathematical problems, their session key could be broken when the telecare server *S*'s secret private key is revealed. Additionally, according to above analysis, the security of

Mishra et al.'s scheme [26] entirely replies on the patient's real identity. However, the patient's identity can be leaked in various ways, so Mishra et al.'s scheme [26] could not provide a proper security at an acceptable level for TMIS in practice.

IV. OUR PROPOSED SCHEME

As demonstrated in Section V, Mishra et al.'s scheme [26] fails to achieve the claimed security goals since an adversary can perform a guessing attack to obtain the patient's real identity and then she/he can launch various attacks successfully. In addition, their scheme could not provide perfect forward secrecy since the security of their scheme was independent on the intractable mathematical problems. In order to erase above security weaknesses, we present an improved authentication scheme by combining the three-factor authentication technology with the chaotic map-based cryptography.

Firstly, we review the basics of Chebyshev chaotic maps briefly. For more details, please refer to [46, 47].

Chebyshev polynomial $T_n(x):(-\infty,+\infty)\to[-1,+1]$ defined as $T_n(x)=(2xT_{n-1}(x)-T_{n-2}(x)) \bmod p$, where $x\in(-\infty,+\infty)$, n is an integer, $n\geq 2, T_0(x)=1, T_1(x)=x$, and p is a large prime number. The Chebyshev polynomial satisfies the semi-group property: $T_{uv}(x)=T_v(T_u(x))=T_u(T_v(x))$, where $u,v\in N$ and $x\in(-\infty,+\infty)$.

Definition 1 Chaotic Map Discrete Logarithm problem (CMDLP): Given two elements y and x, it is computationally infeasible to find an integer u such that $T_u(x)=y$.

Definition 2 Chaotic Map Computational Diffie-Hellman problem (CMCDHP): Given $x, T_u(x), T_v(x)$, it is computationally infeasible to compute $T_{uv}(x)=y$.

We assume that above two problems are intractable. That is, there is no polynomial time algorithm solving these problems with non-negligible probability.

Next, we describe the proposed chaotic map-based three factor authenticated key agreement scheme in detail. The proposed scheme consists five phases: initialization phase, registration phase, login phase, authentication phase, and password and biometrics update phase.

A. Initialization phase

In this phase, the telecare server *S* chooses a high entropy integer *x* randomly, a high entropy random integer *mk* as a master key, a secure one-way hash function *h*(.) and a symmetric key cryptosystem (such as AES-256) with the encryption algorithm E_k(.) and a decryption algorithm D_k(.).

B. Registration phase

This phase is executed for a patient who wants to be a legal user in TMIS. All the steps are performed between the patient U_i and the telecare server *S* via a secure channel. The detail of the registration phase described as follows and illustrated in Fig. 2.

*Step R*1: the patient U_i freely selects its identity ID_i , its password PW_i, and imprints its biometrics B_i via a sensor. Next, it generates a high entropy random integer N_i, and then computes $PB_i = B_i \oplus N_i$, $W_i = ID_i \oplus PW_i \oplus PB_i$, $V_i = h(ID_i \oplus PW_i) \oplus N_i$, $Z_i = h(ID_i \oplus PW_i \oplus N_i) \oplus PB_i$, where PB_i is used to protect the patient's biometrics from being compromised in case of the smart card is lost or stolen. Finally, the patient U_i sends the registration request message $\{ID_i, W_i\}$ to the telecare server *S*.

*Step R*2: after receiving the message $\{ID_i, W_i\}$, the telecare server *S* records ID_i into the identity table and then chooses a random integer *R* to generate U_i's dynamic identity *NID*= $E_{mk}(ID_i \| R)$. Next, it computes $X_i = h(ID_i \| mk)$, $Y_i = X_i \oplus W_i$ and then writes $\{NID, Y_i, h(.), x\}$ into the smart card. Finally, the telecare server *S* issues the smart card to the patient U_i.

*Step R*3: upon receiving the smart card, the patient U_i stores the parameters $\{Z_i, V_i\}$ into it secretly. Finally, the smart card contains $\{NID, Y_i, Z_i, V_i, h(.), x\}$.

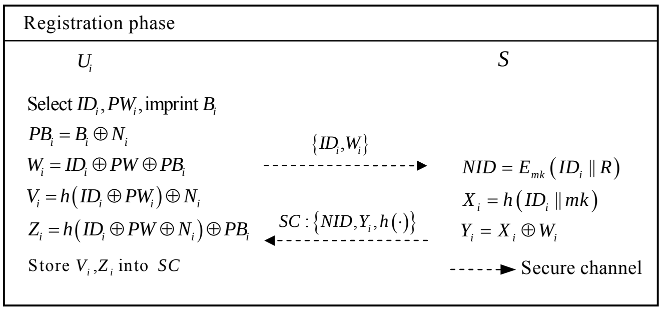
Registration phase
U_i
S
Select ID_i, PW_i, imprint B_i
$PB_i = B_i \oplus N_i$
$W_i = ID_i \oplus PW \oplus PB_i$
$V_i = h(ID_i \oplus PW_i) \oplus N_i$
$Z_i = h(ID_i \oplus PW \oplus N_i) \oplus PB_i$
Store V_i, Z_i into SC
$\{ID_i, W_i\}$
$SC : \{NID, Y_i, h(\cdot)\}$
$NID = E_{mk}(ID_i \| R)$
$X_i = h(ID_i \| mk)$
$Y_i = X_i \oplus W_i$
Secure channel

Fig. 2 The pictorial representation of registration phase

C. *Login phase*

In the login phase, the patient U_i performs following steps as shown in Fig. 3.

*Step L*1: the patient U_i inserts its smart card into the card reader and then it inputs its identity ID_i , its password PW_i and imprints its biometrics B_i^* via a sensor.

*Step L*2: the smart card computes $N_i = V_i \oplus h(ID_i \oplus PW_i)$, $PB_i = h(ID_i \oplus PW_i \oplus N_i) \oplus Z_i$ and $PB_i^* = B_i^* \oplus N_i$. Then it compares PB_i^* with PB_i. If the matching score $\Delta(PB_i^*, PB_i)$ is beyond a predefined threshold value, the smart card terminates the login phase. Otherwise, it proceeds to next step.

*Step L*3: the smart card chooses a random integer u, and then it computes $T_u(x), W_i = ID_i \oplus PW_i \oplus PB_i, X_i = Y_i \oplus W_i$, and $a_i = h(ID_i \| X_i \| T_u(x))$. Next, it sends the login request message $m_1 = \{NID, a_i, T_u(x)\}$ to the telecare server S over a public channel.

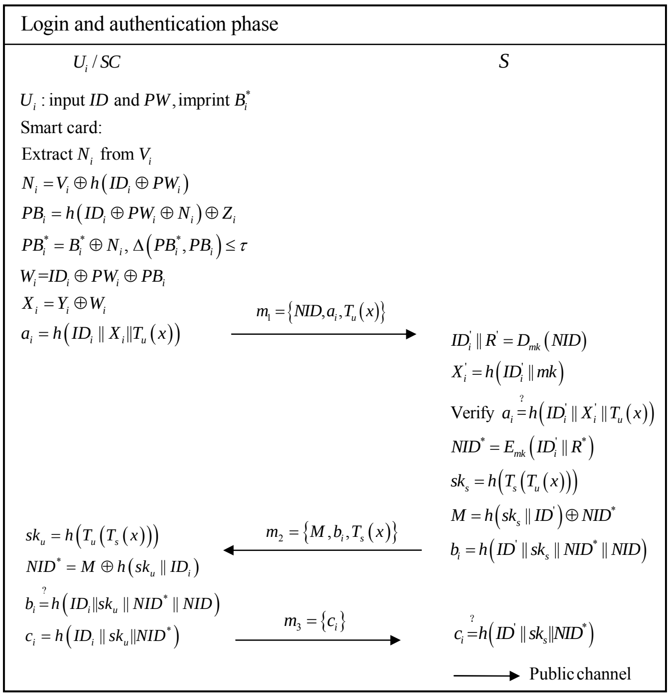
Login and authentication phase
U_i / SC
S
U_i : input ID and PW, imprint B_i^*
Smart card:
Extract N_i from V_i
$N_i = V_i \oplus h(ID_i \oplus PW_i)$
$PB_i = h(ID_i \oplus PW_i \oplus N_i) \oplus Z_i$
$PB_i^* = B_i^* \oplus N_i, \Delta(PB_i^*, PB_i) \le \tau$
$W_i = ID_i \oplus PW_i \oplus PB_i$
$X_i = Y_i \oplus W_i$
$a_i = h(ID_i \| X_i \| T_u(x))$
$m_1 = \{NID, a_i, T_u(x)\}$
$ID_i' \| R' = D_{mk}(NID)$
$X_i' = h(ID_i' \| mk)$
Verify $a_i \overset{?}{=} h(ID_i' \| X_i' \| T_u(x))$
$NID^* = E_{mk}(ID_i' \| R^*)$
$sk_s = h(T_s(T_u(x)))$
$M = h(sk_s \| ID') \oplus NID^*$
$b_i = h(ID' \| sk_s \| NID^* \| NID)$
$m_2 = \{M, b_i, T_s(x)\}$
$sk_u = h(T_u(T_s(x)))$
$NID^* = M \oplus h(sk_u \| ID_i)$
$b_i \overset{?}{=} h(ID_i \| sk_u \| NID^* \| NID)$
$c_i = h(ID_i \| sk_u \| NID^*)$
$m_3 = \{c_i\}$
$c_i \overset{?}{=} h(ID' \| sk_s \| NID^*)$
Public channel

Fig. 3 The pictorial representation of login and authentication phases

D. *Authentication phase*

After receiving the login message, the telecare server *S* and the smart card perform the following steps to achieve mutual authentication and key agreement as shown in Fig. 3.

*Step A*1: the telecare server *S* retrieves *U_i*'s original identity by decrypting *NID* via the master key *mk* and checks whether the extracted identity ID_i' is valid according to the identity table. If not, *S* terminates the session. Otherwise, it computes $X_i' = h(ID' \| mk)$ and verifies whether the following equation holds $a_i = h(ID_i' \| X_i' \| T_u(x))$. If not, the process stops, otherwise *S* generates two random integers R^* and *s* to generate a new dynamic identity $NID^* = E_{mk}(ID_i' \| R^*)$. And then it calculates the shared session key $sk_s = h(T_s(T_u'(x)))$. Next, the telecare server *S* computes $M = h(sk_s \| ID_i') \oplus NID^*$ and $b_i = h(ID_i' \| sk_s \| NID^* \| NID)$, and then it deliveries $m_2 = \{b_i, M, T_s(x)\}$ to the patient U_i via a public channel.

*Step A*2: after receiving the message *m*2, the smart card computes $sk_u = h(T_u(T_s(x)))$ to retrieve the dynamic identity $NID^* = M \oplus h(sk_u \| ID_i)$ and then checks whether the value of *bi* is equivalent to $h(ID_i \| sk_u \| NID^* \| NID)$. If they are not equal, the smart card stops this session. Otherwise, the patient *Ui* believes that the telecare server *S* is a legal server and then it replaces the old *NID* by NID^*. At last, the smart card computes $c_i = h(ID_i \| sk_u \| NID^*)$ and submits $m_3 = \{c_i\}$ to the telecare server *S* via a public channel.

*Step A*3: upon receiving the message *m*3, the telecare server *S* computes $h(ID_i^{'} \| sk_u \| NID^*)$ and checks if the result is equal to *ci*. If the verification dissatisfies, it terminates this session, otherwise, the telecare server *S* believes that the patient *Ui* is a legal patient and sets the *sks* as their shared session key.

E. Password and biometrics update phase

This phase enables the legal patient *Ui* change its password and biometrics without communication with the telecare server *S* as shown in Fig. 4.

*Step P*1: the patient *Ui* inserts its smart card into the card reader. And then it inputs its identity *IDi* , its password *PWi* and imprints its biometrics B_i^* via a sensor.

*Step P*2: the smart card computes $N_i = V_i \oplus h(ID_i \oplus PW_i)$,

$PB_i = h(ID_i \oplus PW_i \oplus N_i) \oplus Z_i$ and $PB_i^* = B_i^* \oplus N_i$. Then it compares PB_i^* with *PBi* If the matching score $\Delta(PB_i^*, PB_i)$ is beyond a predefined threshold value, the smart card rejects this request .Otherwise, the smart card returns the message (*Request new password and biometrics*) to the patient *Ui*.

*Step P*3: the patient *Ui* selects a new password PB_i^{new}, a new random integer N_i^{new}, and imprints a new biometrics B_i^{new} via a sensor.

*Step P*4: upon receiving the new parameters, the smart card computes $PB_i^{new} = B_i^{new} \oplus N_i^{new}$, $Y_i^{new} = Y_i \oplus PW_i \oplus PW_i^{new} \oplus PB_i \oplus PB_i^{new}$, $V_i^{new} = h(ID_i \oplus PW_i^{new} \oplus N_i^{new})$, $Z_i^{new} = h(ID_i \oplus PW_i^{new} \oplus N_i^{new}) \oplus PB_i^{new}$ and replaces the old parameters with $(Y_i^{new}, V_i^{new}, Z_i^{new})$, respectively.

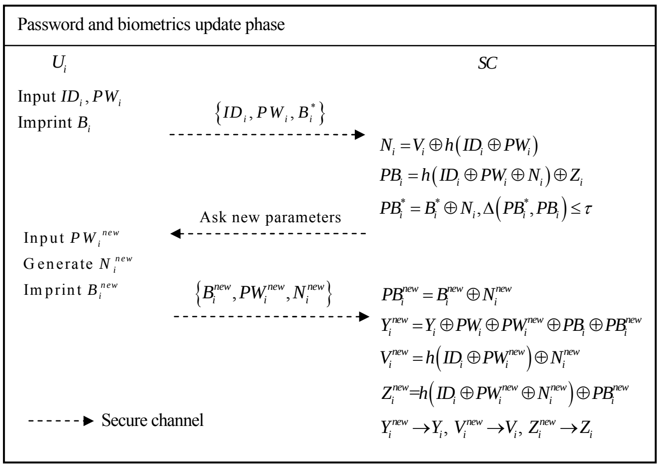
Password and biometrics update phase
U_i
SC
Input ID_i, PW_i
Imprint B_i
$\{ID_i, PW_i, B_i^*\}$
$N_i = V_i \oplus h(ID_i \oplus PW_i)$
$PB_i = h(ID_i \oplus PW_i \oplus N_i) \oplus Z_i$
$PB_i^* = B_i^* \oplus N_i, \Delta(PB_i^*, PB_i) \le \tau$
Ask new parameters
Input PW_i^{new}
Generate N_i^{new}
Imprint B_i^{new}
$\{B_i^{new}, PW_i^{new}, N_i^{new}\}$
$PB_i^{new} = B_i^{new} \oplus N_i^{new}$
$Y_i^{new} = Y_i \oplus PW_i \oplus PW_i^{new} \oplus PB_i \oplus PB_i^{new}$
$V_i^{new} = h(ID_i \oplus PW_i^{new}) \oplus N_i^{new}$
$Z_i^{new} = h(ID_i \oplus PW_i^{new} \oplus N_i^{new}) \oplus PB_i^{new}$
Secure channel
$Y_i^{new} \to Y_i,\ V_i^{new} \to V_i,\ Z_i^{new} \to Z_i$

Fig. 4 The pictorial representation of password and biometrics update phases

V. Security analysis

This section analyzes the security and functionality of our proposed scheme. Following the attack model defined in Section III, the adversary Eve can compromise the message $\{NID, Y_i, Z_i, V_i, h(\cdot), x\}$ stored in the smart card and record all the messages transmitted between the patient and the telecare server. Detailed analysis is described in this section.

A. Replay attacks

Suppose that an adversary *Eve* records the login request message m_1 and replays it to the telecare server *S* intending to impersonate the patient U_i. However *Eve* cannot construct a valid $c_i = h(ID_i \| sk_u \| NID^*)$ to pass the verification process of the telecare server *S* unless she can correctly guess the shared session key sk_u, the identity ID_i and the new dynamic identity NID^* .However, when *Eve* tries to compute the session key sk_u by using the intercepted message $T_s(x)$,previous intercepted message $T_u(x)$ and the random integer *x* stored in the smart card, she will face the Chaotic Map Computational Diffie-Hellman problem (CMCDHP). In addition, *Eve* also cannot extract the sk_s from the obtained message b_i, since sk_s is protected by a secure hash function. Moreover, the patient identity ID_i is protected by a secure one way hash function during the communication process, so the adversary *Eve* cannot extract ID_i from the intercepted message. Furthermore, *Eve* cannot compromise the new dynamic identity $NID^* = E_{mk}(ID_i^{'} \| R)$ without the knowledge of patient identity $ID_i^{'}$, high entropy random integer *R* and the telecare server *S*'s master key *mk*. On the other hand, assume that the adversary *Eve* intercepts the login request message and replays a previous message m_2 to the patient U_i. For the same reason, the adversary cannot construct a valid session key b_i to pass the verification possess of patient U_i. So, the patient U_i will detect this replay attack easily by comparing the received b_i and its computed value $h(ID_i \| sk_u \| NID^* \| NID)$ .Therefore, the proposed scheme can withstand the replay attack.

B. Modification attacks

Suppose that the adversary *Eve* modifies $T_u(x)$ to $T_u^*(x)$ and sends $\{NID, a_i, T_u^*(x)\}$ to the telecare server *S* to impersonate the patient U_i. However, *S* can detect this attack by checking whether or not $a_i = h(ID_i^{'} \| X_i^{'} \| T_u(x))$ holds. If the adversary *Eve* wants to pass the telecare server's verification, she needs to construct a valid $a_i^* = h(ID_i^{'} \| X_i^{'} \| T_u^*(x))$ .However *Eve* cannot obtain $X_i^{'}$ without the knowledge of the master key *mk* and the patient identity ID_i. In addition, she cannot calculate the valid $X_i^{'}$ by using the message Y_i stored in the smart card without the knowledge of (ID_i, PW_i, PB_i).

Assume that an adversary *Eve* modifies the message $\{b_i, M, T_s^*(x)\}$ and sends it to the patient U_i. Similarly, *Eve* needs to construct a valid $b_i^* = h(ID_i^{'}\|sk_s^*\|NID^* \| NID)$ to pass the verification of the patient U_i. For the same reason discussed in the subsection 6.1, the adversary *Eve* will face the Chaotic Map Computational Diffie-Hellman problem (CMCDHP).

If an adversary *Eve* forges the message c_i' and sends it to the telecare server *S* to impersonate the patient U_i. The telecare server *S* can find out that c_i' is not equivalent to its computed value, since *Eve* cannot correctly guess the value of *sk*, ID_i and *NID*. Therefore, the proposed scheme can resist the modification attack.

C. Man-in-the-middle attacks

In the proposed scheme, a session key *sk* can be shared only after mutual authentication between the patient U_i and the telecare server *S*. Therefore, if an adversary *Eve* attempts to make the telecare server *S* believes that it is talking to the patient U_i, she needs to pass the verification of *S*. However, for the same reason mentioned above *Eve* cannot pass this process without the knowledge of patient's ID_i and the secret value X_i. On the other hand, *Eve* also cannot construct a valid b_i to pass the patient's verification without knowing the message (ID_i, sk_s, NID^*). So, the adversary cannot cheat the patient U_i to share a session key and make it believe that the key is shared with the telecare server *S*, and this judgment also works on *S*. Therefore, the adversary cannot launch the man-in-middle attack successfully to cheat either the patient or the telecare server in the proposed scheme.

D. Password guessing attacks with smart card

Assume that an adversary *Eve* compromises the message {*NID*, Y_i, Z_i, V_i, *h*(.), *x* }stored in the smart card and then tries to guess the patient's password. However, *Eve* cannot correctly guess the password by using the compromised message V_i

and $Z_i = h(ID_i \oplus PW_i \oplus N_i) \oplus PB_i = h(ID_i \oplus PW_i \oplus V_i \oplus h(ID_i \oplus PW_i)) \oplus B_i \oplus V_i \oplus h(ID_i \oplus PW_i)$, since the password is protected by the patient identity ID_i and the biometric data B_i. Without the privacy message of the patient, *Eve* cannot determine whether the guessed password is correct or not. In addition, *Eve* cannot guess the patient U_i's password from $Y_i = X_i \oplus W_i = h(ID_i \| mk) \oplus ID_i \oplus PW_i \oplus PB_i$ without the knowledge of ID_i, B_i and the master key *mk*. Therefore, the adversary cannot launch the password guessing attacks with the smart card successfully in the proposed scheme.

E. Privileged-insider attacks

The proposed scheme can resist the privileged-insider attack. That because in the registration phase, the patient U_i's password is protected by its identity ID_i, its biometric data B_i and a high entropy random integer N_i. So a malicious privileged-insider in the telecare server cannot obtain the patient's password during the registration phase.

F. Insider impersonation attacks

Assume that the patient U_A is a malicious patient who attempts to impersonate patient U_i to establish a session with the telecare server *S*. Since the patient U_A is a legal user, it can go through the login process successfully. First, the patient U_A use its privacy message to pass the verification and then it U_A computes $a_A = h(ID_i \| X_A \| T_u(x))$ via patient U_i's identity, and then sends message $\{NID_A, a_A, T_u(x)\}$ to the telecare server *S*. However this attack can be found easily, when the telecare server *S* checks the equation $a_S = h(ID'_A \| X'_A \| T_u(x)) \neq a_A$. That because, the ID_i in the message a_A is patient U_i's identity and the ID'_A computed in the a_s is from U_A. So, the value of (ID_i, X_A) in a_A are not equal to the value of (ID'_A, X'_A) in the a_s respectively. Therefore, in the proposed scheme, a legal but malicious patient cannot impersonate other legitimate patient to access to the telecare server.

G. Stolen smart card attacks

Suppose that an adversary *Eve* compromises the secret message {*NID*, Y_i, Z_i, V_i, *h*(.), *x* } stored in the smart card and eavesdrops transmitted messages from the public network. In order to establish an authorized session with the telecare server *S*, *Eve* needs to generate a valid $a_i = h(ID_i \| X_i \| T_u(x))$ to pass the login verification. For the same reason discussed in the subsection *A Replay attack*, *Eve* cannot calculate a valid a_i without the knowledge of the master key *mk* and the patient identity ID_i or the message ID_i, PW_i, and PB_i. Therefore, in the proposed scheme, even if an adversary had stolen the patient's smart card, it could not login on the telecare server via the compromised message stored in the smart card.

H. Known Session Specific Temporary Information Attacks

If the session key depends only on the secrecy of randomly generated values, it may cause a known session specific temporary information attacks [37]. In our scheme, the session key was calculated by the identity, the secret value X_i and the randomly generated values (*u*, *s*), so the proposed scheme can withstand the known session specific temporary information attack.

I. Session key security

In the proposed scheme, only the patient U_i and the telecare server *S* can calculate the session key $sk = h(T_s(T_u(x)))$ $= h(T_u(T_s(x)))$ since the random integer *u* and *s* generated by the patient U_i and the telecare server *S* are different in every session. In addition, since the session key *sk* is protected by a secure one way hash function, the adversary cannot obtain it from the intercepted b_i or c_i. Furthermore, even if an adversary obtains the message $T_u(x)$ and $T_s(x)$ from the public channel, and then compromise the secret *x* from the smart card, she could not calculate the session key *sk* due to the hardness of CMDLP. Therefore, the proposed scheme achieves session key security.

J. Known-key security

An authentication scheme could provide known-key security if its execution could generate a unique session key and the compromise of this key has no impact on other session keys. In the proposed scheme, the session key $sk = h(T_s(T_u(x))) \quad = h(T_u(T_s(x)))$ is unique in each run of the authentication scheme. That because the random integer *u* and *s* are generated randomly and independently by the patient U_i and the telecare server *S* respectively. So, in the proposed scheme, the compromised session key has no impact on others session keys since the session keys are different in every session. Therefore, the proposed scheme can provide known- key security.

K. Perfect forward secrecy

An authentication scheme could provide perfect forward secrecy if the previous session keys cannot be compromised even both patient and telecare server's secret keys are compromised. In the proposed scheme, the long-term secret key of the telecare *S* is the master key *mk*, and that of the patient U_i is the password PW_i and the secret values $\{Y_i, Z_i, V_i, x\}$ stored in the smart card. Assume that all the secrets mentioned above are compromised by an adversary *Eve*. When trying to calculate previous session key $sk = h(T_u(T_s(x)))$ with the message ($T_s(x)$, $T_u(x)$, x), *Eve* will face the Chaotic Map Computational Diffie-Hellman problem (CDHP). Therefore, without the knowledge of the high entropy random integer *u* and *s*, the adversary *Eve* cannot figure out the previous session key. So, the proposed scheme can provide perfect forward secrecy.

L. User anonymity

An authentication scheme could provide user anonymity if there is no adversary can compromise the patient's identity by launching active or passive attacks in every phase. In the proposed scheme, any adversary cannot compromise the patient's identity by launching active or passive attacks in every phase. In the registration phase, the identity of the patient U_i is protected by its password, its biometric data and a high entropy random integer, so the adversary *Eve* cannot obtain the patient's real identity. During the login and authentication phase, the patient's real identity is protected by a secure one way hash function and a secure symmetric encryption algorithm. Since there are no message need to be transmitted in the password and biometric update phase, the adversary cannot obtain the patient's real identity throughout updating process. More- over, the adversary *Eve* cannot launch a guessing attack to obtain the patient U_i's identity in the proposed scheme. That because, without the knowledge of X_i, *Eve* cannot guess ID_i via $a_i = h(ID_i \| X_i \| T_u(x))$ successfully. So the adversary *Eve* cannot determine whether the guessed identity is correct or not. Similarly, *Eve* cannot obtain the correct identity by using the intercepted message $b_i = h(ID_i' \| sk_s \| NID^* \| NID)$ or $c_i = h(ID_i \| sk_s \| NID^*)$, since she has no capability to calculate sk_s or sk_u from the message ($T_s(x)$, $T_u(x)$, x) due to the hardness of CMDLP. Therefore, in the proposed scheme, nobody can know the real identity of the patient, except the patient himself and the telecare server.

M. User untraceability

In the proposed scheme, to further protect the patient's real identity, the dynamic identity is changed by updating R during every session. Furthermore, the messages transmitted during the communication process in current session are also different with those of other session, since the random integer u and s are chosen randomly and differently in every session. Therefore, an adversary cannot distinguish whether two intercepted messages belong to the same patient or not. So, the proposed scheme provides the user untraceability.

N. Mutual authentication

In the proposed scheme, the telecare server S and the patient U_i can authenticate each other by checking c_i and b_i, respectively. Therefore, the proposed scheme can achieve mutual authentication.

O. Efficient login phase

An authentication scheme achieves efficient login phase if the smart card can identify the incorrect input. In our scheme, assume that an adversary *Eve* compromise the patient U_i's identity ID_i and its password PW_i , and then it tries to login to the telecare server S, this illegal login will be detect by comparing the value of PB_i^* and PB_i. Without the knowledge of patient's biometric data B_i, the matching score of $\Delta(PB_i^*, PB_i)$ will beyond a predefined threshold value. Then the smart card aborts the login session.

On the other hand, if the patient U_i inputs a wrong ID_i or PW_i by accident, the login session will be also terminated even the biometric data is correct. Since the message PB_i is constructed by patient's biometric data B_i and a random integer N_i which can be calculate by secret V_i, identity ID_i and password, PW_i the wrong input of password or identity will cause the matching score of $\Delta(PB_i^*, PB_i)$ beyond a predefined threshold value. Consequently, the smart card will abort the login request. Therefore, the proposed scheme achieves efficient login phase.

P. User friendly and efficient password and biometrics changes phase

In the proposed scheme, the patient is allowed to change her/his password and biometrics freely without the telecare server's assistance which makes the proposed scheme user-friendly. Since the smart card can verify the correctness of the input efficiently, a patient can change her/his password and biometrics correctly and efficiently.

Q. Biometrics protection

In the proposed scheme, the patient's biometric data is protected by a high entropy random integer N_i. So, even if the adversary obtains the smart card, she cannot retrieve the patient U_i's biometric without the knowledge of the patient U_i's identity ID_i and password PW_i. Therefore, the proposed scheme provides the biometrics protection.

VI. Scheme Evaluation

In this section, we first compare the security attributes of our proposed scheme with Mishra et al.'s scheme [26], Amin et al.'s scheme [28], Xu et al.'s [16] scheme, and other chaotic map-based authentication and key agreement schemes such as Lee [34], Mishra [35]. TABLE II lists security attributes comparisons between our proposed scheme and other related schemes.

TABLE II

Security attributes comparison with other pertinent authentication schemes

Security attributes	Lee [34]	Mishra [35]	Xu [16]	Mishra [26]	Amin [28]	Ours
Replay attacks	√	√	√	×	√	√

Smart card theft attacks	√	√	√	×	√	√
Modification attacks	√	√	√	×	√	√
Man-in-the-middle attacks	√	√	√	×	√	√
Password guessing attacks	√	√	√	√	√	√
Privileged-insider attacks	√	√	√	√	√	√
Insider impersonation attacks	√	√	√	√	√	√
Known session specific temporary information attack	√	√	√	√	×	√
Denial of	×	√	×	√	√	√

service attacks						
User anonymity	√	√	√	×	√	√
User untraceability	√	√	√	×	√	√
Mutual authentication	√	√	√	×	√	√
Session key security	√	√	√	×	√	√
Perfect forward secrecy	√	×	√	×	√	√
Efficient login and password and biometrics change phase	×	×	×	√	√	√
User-friendl	×	×	×	√	√	√

y password change						
Biometrics protection	-	-	-	√	×	√

As shown in TABLE II, the proposed scheme is secure against various attacks while provides many attractive features such as user anonymity, perfect forward secrecy, efficient login and password updating, which have not been considered or provided by other related schemes. Although Amin and Biswas's scheme [28] also fixed the limitations of Mishra et al.'s scheme [26], their scheme suffered from the known session specific temporary information attack. Furthermore, since Amin and Biswas's scheme [28] do not provide biometrics protection, the adversary could retrieve the patient U_i's biometric template directly through obtaining the smartcard.

Then, we compared the computational cost of our scheme with other relevant schemes as listed in TABLE III, where T_C, T_H, T_h , T_E, T_A and T_s are the time complexity of the Chebyshev map operation, the Biohashing operation, the one-way hash operation, the scalar multiplication operation of elliptic curve, the point addition operation of elliptic curve, the symmetric key encryption/decryption operations, respectively. It is noted that the XOR operation is ignored because it's running time is negligible.

Compared with Chebyshev map and symmetric encryption/ decryption operations, the time complexity for one-way hash operation is very lightweight. TABLE III shows that the computational overhead of our scheme is lower than Mishra et al.'s [35], Xu et al.'s [16] and Amin et al.'s [28] schemes. Although Lee [34] and Mishra et al.'s schemes [26] are efficient than our proposed scheme, their scheme is vulnerable to some malicious attacks.

Furthermore, Mishra et al.'s scheme [26], Amin et al.'s scheme [28] and our proposed scheme require three times of message exchange to achieve mutual authentication and session key agreement whileas Xu et al.'s scheme [16] and other two chaotic map-based schemes [34, 35] need two times to finish mutual authentication and session key agreement. Furthermore, due to the usage of timestamps, these schemes will face the clock synchronization problem, which is difficult and expensive to be solved in TMIS environments [48]. Obviously, employing a timestamp mechanism to resist the replay attack is not suitable for TMIS. Therefore, the proposed scheme achieves a delicate balance between security and performance for TMIS in comparison with other related works.

TABLE III

Performance comparisons with other relevant authentication schemas

Phases	Lee [34]	Mishra[35]	Xu [16]	Mishra [26]	Amin [28]	Ours
Registration	$4T_h$	T_C+ $2T_h$	$1T_E$	T_H+T_s +$3T_h$	T_H+T_s + $3T_h$	T_s+$3T_h$
Login	$1T_C$+ $3T_h$	$2T_C$ + $4T_h$	$2T_E$ + $3T_h$	T_H+ $3T_h$	T_E+T_H + $3T_h$	T_C+ $3T_h$
Authentication	$3T_C$+ $8T_h$	T_C+ $6T_h$	$3T_E$ + $7T_h$	$2T_s$+ $10T_h$	$4T_E$+2 T_{As}+8 T_h+2T	$3T_C$+2 T_s +$10T_h$

					s	
Password&biometrics update	$4T_h$	$3T_C+11T_h$	$2T_h$	$2T_H+4T_h$	T_H+3T_h	$4T_h$
Total	$4T_C+19T_h$	$6T_C+23T_h$	$6T_E+14T_h$	$4T_H+3T_s+20T_h$	$5T_E+2T_A+3T_H+17T_h+3T_s$	$4T_C+3T_s+20T_h$
Communication round	2	2	2	3	3	3

In TABLE IV, we summarize the communication costs of our scheme and other related schemes. We assumes that the length of the hash function output digest, nonce, user identity, Chebyshev chaotic map and timestamp is 160-bit. To achieve 1024-bit RSA level security, a 160-bit ECC key is employed. The length of key for symmetric encryption/decryption is 256-bit. From TABLE IV, we conclude that our proposed scheme is more efficient than Lee's scheme [34], Xu et al.'s scheme [16] and Amin et al.'s scheme [28], and as efficient as Mishra et al.'s scheme [26] in communication overhead. Although the communication overhead of our scheme is slightly higher than Mishra et al.'s [35], our scheme avoids using timestamps and can resist various attacks and provide more security properties. Therefore, the proposed scheme achieves a delicate balance between security and performance for TMIS in comparison with other related schemes.

TABLE IV

Communication overhead comparisons with other relevant authentication schemes

scheme	Login phase	Authentication phase	Total
Lee [34]	800 bits	800 bits	1600 bits
Mishra[35]	640 bits	320 bits	960 bits
Xu et al. [16]	800 bits	640 bits	1440 bits
Mishra et al.[26]	576 bits	736 bits	1312 bits
Amin et al.[28]	736 bits	896 bits	1632 bits
Ours	576 bits	736 bits	1312 bits

VII. CONCLUSION

In this paper, we have demonstrated that Mishra et al.'s authentication scheme suffers from various attacks and fails to provide several security properties. And then, we have proposed a three-factor authenticated key agreement scheme by using chaotic map-based cryptography to address these problems. The proposed scheme realizes the protection of medical data transmitted in the open channel and provides privacy protection during the remote diagnosing process, which enables the patient to enjoy the secure and convenient healthcare through the TMIS. Security analysis has proved that the proposed scheme can resist various attacks, and performance analysis has shown that the proposed scheme achieves better performance in comparison with other related schemes. Thus, the proposed scheme is more suitable for practical applications in TMIS environments.

ACKNOWLEDGEMENTS

This work was supported by the National Natural Science Foundation of China [grant numbers 61303237, 61272469]; the Wuhan Scientific Research Program [grant number 2013010501010144]; China Postdoctoral Fund [grant number 2012194091]; the Fundamental Research Funds for the Central Universities [grant number 2013199037]; and Teaching Laboratory Open Funds of China University of Geosciences [grant number skj2014234].

REFERENCES

[1] S. Li, C. Wang, W. Lu, Y. Lin, D. Yen, “Design and implementation of a telecare information platform”, *J. Med. Syst.,* vol.36, no. 3, pp.1629-1650, 2012.

[2] L. Nguyen, E. Bellucci, “Electronic health records implementation: An evaluation of information system impact and contingency factors”, *Int. J. Med. Inf.*, vol. 83, no. 11, pp. 779-796, 2014.

[3] V.L. Patel, J.F. Arocha, A.W. Kushniruk, “Patients’ and Physicians’ understanding of health and biomedical concepts: relationship to the design of EMR systems”, *J. Biomed. Inform.*, vol. 35, pp. 8–16, 2002.

[4] J. Scholl, S. Syed-Abdul, A.L. Ahmed, "A case study of an EMR system at large hospital in India: challenges and strategies for successful adoption", *J. Biomed. Inform.*, vol. 44, pp. 958–967,2011.

[5] C. Esposito, M. Ciampi, G. Pietro, "An event-based notification approach for the delivery of patient medical information", *Inform. Syst.*, vol.39, pp. 22-44, 2014.

[6] P. Accenture, "Overview of International EMR/EHR Markets: Results from a Survey of Leading Health Care Companies", http://www.accenture.com au-en/Pages/insight-electronic-medical-record-survey-summary.aspx, 2010.

[7] G. Perera, A. Holbrook, L. Thabane, G. Foster, D. Willison, "Views on health information sharing and privacy from primary care practices using electronic medical records", *Int. J. Med. Inf.*, vol. 80, no. 2, pp. 94-101, 2011.

[8] J. Hur, K. Kang, "Dependable and secure computing in medical information systems", *Comput. Commu.*, vol. 36, no. 1, pp. 20-28, 2012.

[9] C.D. Lee, K.I. Ho, W.B. Lee, "A novel key management solution for reinforcing compliance with HIPAA privacy/security regulations", *IEEE Trans. Inf. Technol. Biomed.*, vol.15, pp. 550–556, 2011.

[10] W. Ludwig, K.H. Wolf, C. Duwenkamp, N. Gusew, N. Hellrung, M. Marschollek, M. Wagner, R. Haux, "Health-enabling technologies for the elderly – an overview of services based on a literature review", *Comput. Methods Progr. Biomed.*, vol.106, no. 2, pp.70–78, 2012.

[11] W.B. Lee, C.D Lee, K.I. Ho, "A HIPAA-compliant key management scheme with revocation of authorization", *Comput. Methods Progr. Biomed.*, vol. 113, no. 3, pp. 809–814, 2014.

[12] V. Slavov, P. Rao, S. Paturi, T.K. Swami, M. Barnes, D. Rao, R. Palvai. “A new tool for sharing and querying of clinical documents modeled using HL7 Version 3 standard”, *Comput. Methods Progr. Biomed.*, vol. 112, no. 3, pp. 529–552, 2013.

[13] Y.C. Yu, T.W. Hou, “An efficient forward-secure certificate digital signature scheme to enhance EMR authentication process”, *Med. Biol. Eng. Comput.*, vol.52, pp. 449–457, 2014.

[14] T.F. Lee, C.M. Liu, “A secure smart-card based authentication and key agreement scheme for telecare medicine information systems”, *J. Med. Syst.*, vol. 37, no. 3, pp. 1-11, 2013.

[15] T.F. Lee, “Verifier-based three-party authentication schemes using extended chaotic maps for data exchange in telecare medicine information systems”, *Comput. Methods Progr. Biomed.*, vol. 117, no.3, pp. 464-472, 2014.

[16] X. Xu, P. Zhu, Q.Y. Wen, Z.P. Jin, H. Zhang, L. He, “A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information system”, *J. Med. Syst.*, vol. 38, no. 1, pp. 1-7, 2014.

[17] F.T. Wen, L.D. Guo, “An improved anonymous authentication scheme for telecare medical information systems”, *J. Med. Syst.*, vol. 38, no. 5, pp. 1-8, 2014.

[18] M. Farash, M. Attari, “An efficient and provably secure three-party password-based authenticated key exchange protocol based on Chebyshev chaotic maps”, *Nonlinear Dyn*, vol. 77, no. 1-2, pp. 399-411, 2014.

[19] D. Mishra, “Understanding Security Failures of Two Authentication and Key Agreement Schemes for Telecare Medicine Information Systems”. *J. Med. Syst*, doi: 10.1007/s10916-015-0193-7, 2015..

[20] N. Radha, S. Karthikeyan, “A study on biometric template security”, *ICTACT J Soft Comput.*, vol. 1, no. 1, pp. 37-41, 2010.

[21] A. Awasthi, K. Srivastava, “A biometric authentication scheme for telecare medicine information systems with nonce”, *J. Med. Syst.*, vol. 37, no. 5, pp. 1-7, 2013.

[22] D. Mishra, S. Mukhopadhyay, S. Kumari, M. Khan, A. Chaturvedi., “Security enhancement of a biometrics based authentication scheme for telecare medicine information systems with nonce”, *J. Med. Syst.*, vol. 38, no. 5, pp. 1-11, 2014.

[23] Z. Tan. “A user anonymity preserving three-factor authentication scheme for telecare medicine information systems”, *J. Med. Syst.*, vol. 38, no. 3, pp. 1-9, 2014.

[24] H. Arshad, M. Nikooghadam, “Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems”, *J. Med. Syst.*, vol. 38, no. 3, pp. 1-9, 2014.

[25] X. Yan, W. Li, P. Li, J. Wang, X. Hao, P. Gong, “A secure biometrics-based authentication scheme for telecare medicine information systems”, *J. Med. Syst.*, vol. 37, no. 5, pp. 1-6, 2013.

[26] D. Mishra, S. Mukhopadhyay, A. Chaturvedi, S. Kumari, M. Khan, “Cryptanalysis and improvement of Yan et al.’s biometric-based authentication scheme for telecare medicine information systems”, *J. Med. Syst.*, vol. 38, no. 6, pp. 1-12, 2014.

[27] Mrudula Sarvabhatla, M. Giri, Chandra Sekhar Vorugunti, “Cryptanalysis of cryptanalysis and improvement of Yan et al. biometric- based authentication scheme for TMIS”, CoRR, 2014. arXiv:1406.3943.

[28] R. Amin, G.P. Biswas, “A secure three-factor user authentication and key agreement protocol for tmis with user anonymity”, *J. Med. Syst*, vol. 39, no. 8, 2015.

[29] L.P. Zhang, S.H., Zhu, “Robust ECC-based authenticated key agreement scheme with privacy protection for Telecare Medicine Information Systems”, *Journal of Medical System*, vol. 39, no. 5, pp. 1-13, 2015.

[30] L.P. Zhang, S.Y. Tang, S.H. J. Chen, Zhu, “Two-factor remote authentication protocol with user anonymity based on elliptic curve cryptography”, *Wireless personal communications*, vol. 81, no. 1, pp. 53-75, 2015.

[31] L.P. Zhang, S.Y. Tang, S.H. Zhu, “An energy efficient authenticated key agreement protocol for SIP-based green VoIP networks”, *Journal of Network and Computer Applications*, doi:10.1016/j.jnca.2015.06.022, 2015.

[32] D.B. He, Y. Chen, “Cryptanalysis and improvement of an extended chaotic maps-based key agreement protocol”, *Nonlinear Dyn*, vol. 69, no. 3, pp. 1149-1157, 2012.

[33] F. Zhao, P. Gong, S. Li, M. Li, P. Li, “Cryptanalysis and improvement of a three-party key agreement protocol using enhanced Chebyshev polynomials”, *Nonlinear Dyn*, vol. 74, no. 1-2, pp. 419-427, 2013.

[34] Tian Fu Lee, “An efficient chaotic maps-based authentication and key agreement scheme using smartcards for telecare medicine information systems”, *J. Med. Syst.*, vol. 37, no. 6, pp: 1–9, 2013.

[35] D. Mishra, J. Srinivas, S. Mukhopadhyay, “A Secure and Efficient Chaotic Map-based Authenticated Key Agreement Scheme for Telecare Medicine Information Systems”, *J. Med. Syst*, vol. 38, no. 10, pp. 1-10, 2014.

[36] H. Lin, “Improved chaotic maps-based password authenticated key agreement using smart cards”, *Commun. Nonlinear Sci. Numer. Simul.*, vol. 20 no. 2, pp. 482-488, 2015.

[37] D. Mishra, S. Mukhopadhyay, “Cryptanalysis of Pairing-free Identity Based Authenticated Key Agreement Protocols”, *9th International Conference on Information Systems Security* (ICISS 2013), ISI Kolkata, India, LNCS, Vol.8303, pp. 247--254, Springer, December 16-20, 2013.

[38] M. Baptista, “Cryptography with chaos”, *Phys. Lett. A*. vol. 24, no. 1-2, pp. 50-54, 1998.

[39] W. Yau, R. Phan, “Cryptanalysis of a chaotic map-based password-authenticated key agreement protocol using smart cards”, *Nonlinear Dyn.* , vol. 79, no. 2, pp. 809-821, 2015.

[40] Q. jiang, F.S. Wei, J.F. Ma, G.S. Li, A. Alelaiwi, “Robust extended chaotic maps-based three-factor authentication scheme preserving biometric template privacy”, *Nonlinear Dyn.* pp.1-17, 2015.

[41] D. Mishraa, A. K. Dasb, A. Chaturvedic, S. Mukhopadhyayc. “A secure password-based authentication and key agreement scheme using smart cards”, *Journal of Information Security and Applications*, vol. 23, no. 2015, pp. 28-43, 2015.

[42] D. Mishra, “On the Security Flaws in ID-based Password Authentication Schemes for Telecare Medical Information Systems”, *Journal of Medical Systems*, vol. 39, no. 1, pp. 1-16, 2015.

[43] P. Kocher, J. Jaffe, B. Jun, “Differential power analysis”, *Advance in cryptology-CRYPTO’99*, Springer, Berlin, pp. 15-19, 1999.

[44] T. Messages, E. Dabbish, R. Sloan, “Examining smart card security under the threat of power analysis attacks”, *TEEE Trans. on Comput.*, vol. 51, no.5, pp.541-552, 2002.

[45] Y. F. Chang, S. H. Yu, D. R. Shiao, "An uniqueness and anonymity-preserving remote user authentication scheme for connected health care", *J. Med. Syst.* , doi: 10.1007/s10916-012-9902-7, 2013.

[46] P. Bergamo, P. Arco, A. Santis, L. Kocarev, "Security of public key cryptography based on Chebyshev polynomials", *IEEE Trans. Circ. Syst.*, vol. 52, no. 7, pp. 1382-1393, 2005.

[47] L. Zhang, "Cryptanalysis of the public key encryption based on multiple chaotic systems", *Chaos Soliton Fract*, vol. 37, no. 3, pp. 669-674, 2008.

[48] A .Giridhar, P. Kumar, "Distributed clock synchronization over wireless networks: algorithms and analysis", *In: Proceedings of the 45th IEEE conferences on Decision and Control*, IEEE computer society, pp. 4915-4920, 2006.