J Med Syst (2014) 38:136
DOI 10.1007/s10916-014-0136-8

Three-Factor Anonymous Authentication and Key Agreement Scheme for Telecare Medicine Information Systems

Hamed Arshad · Morteza Nikooghadam

Received: 31 May 2014 / Accepted: 22 September 2014 / Published online: 29 October 2014

Abstract Nowadays, with comprehensive employment of the internet, healthcare delivery services is provided remotely by telecare medicine information systems (TMISs). A secure mechanism for authentication and key agreement is one of the most important security requirements for TMISs. Recently, Tan proposed a user anonymity preserving three-factor authentication scheme for TMIS. The present paper shows that Tan's scheme is vulnerable to replay attacks and Denial-of-Service attacks. In order to overcome these security flaws, a new and efficient three-factor anonymous authentication and key agreement scheme for TMIS is proposed. Security and performance analysis shows superiority of the proposed scheme in comparison with previously proposed schemes that are related to security of TMISs.

Keywords Three-factor authentication · Anonymity · Biometric · Key agreement · Telecare medicine information system · Security

Introduction

With the rapid advancement of the internet and information technology, the telecare medicine information systems (TMISs) are more and more employed to provide healthcare delivery services [1]. In fact, the geographical distance between patients and doctors is eliminated by the TMISs. Via the internet, a patient at the home can easily send his/her health information to his/her doctor, or he/she can use portals to access and monitor his/her health information. Security of health data is very important because doctors use this information (e.g. Blood glucose, OXI, EEG, ECG, etc.) to diagnose and treat disease [2, 3]. Since the internet has an open architecture, these systems are prone to various security attacks. A secure and efficient authentication and key agreement scheme is able to provide various aspects of security for health information [4]. Access to the medical servers' resources (e.g. health information) can be controlled by authentication mechanisms, and security of the transmitted data can be provided by encrypting them with the negotiated session keys [4]. Hitherto, many authentication and key agreement schemes have been proposed to provide security in TMIS [1–39].

In 2009, Wang et al. [5] proposed a dynamic ID-based authentication scheme. The term of "dynamic ID-based" means that the identity of the user will change in each session; therefore, the users' activities will be untraceable. However, Wang et al.'s scheme does not provide user anonymity, because the real identity of the user is transmitted over a public channel. Furthermore, Khan et al. [6] pointed out that Wang et al.'s scheme [5] does not provide key agreement and is vulnerable to privileged insider attacks because the server chooses users' passwords. In order to overcome these weaknesses, Khan et al. proposed an improved authentication and key agreement scheme [6]. However, Chen et al. [2] declared that the password change phase of Khan et al.'s scheme [6] does not work properly and their scheme does not provide anonymity. In addition, Chen et al. suggested an improved authentication scheme [2]. Later, Xie et al. [7] showed that in the Chen et al.'s scheme [2] an adversary using a stolen smart card and previous related transmitted messages is able to obtain the user's password and previous established session keys between the user and the server, and also the adversary is able to impersonate a legal user. In addition, Jiang et al. [8]

This article is part of the Topical Collection on *Systems-Level Quality Improvement*

H. Arshad · M. Nikooghadam (✉)
Department of Computer Engineering and Information Technology,
Imam Reza International University, Mashhad, Iran
e-mail: m.nikooghadam@Imamreza.ac.ir

H. Arshad
e-mail: hamedarshad@Imamreza.ac.ir

demonstrated that in the Chen et al.'s scheme [2], an adversary is able to guess the real identity of the user and since the masked identity of the user is static, users' activities are traceable. To overcome these weaknesses, Jiang et al. proposed an enhanced authentication scheme [8]. After that, Wu et al. [9] showed that in the Jiang et al.'s scheme [8], an adversary using a stolen smart card and the previous login messages is able to guess the user's password in an off-line manner. Furthermore, since the inputted password and identity are not checked in the password change phase, if a user mistakenly enters a wrong old password, then he/she will no longer be able to login to the server. Therefore, Jiang et al.'s scheme [8] is vulnerable to denial-of-service attacks [9]. In order to strengthen the security of Jiang et al.'s scheme [8], Wu et al. [9] proposed an improved authentication scheme. However, in [1] it was demonstrated that a legal but malicious user in the Wu et al.'s scheme [9] is able to impersonate the server, obtain the real identity of other users, and guess users' passwords in an off-line manner. Therefore, Wu et al.'s scheme [9] is vulnerable to impersonation attacks and off-line password guessing attacks, and also does not provide user anonymity [1].

In 2012, Wu et al. [10] proposed a new authentication scheme for TMIS. The security of their scheme was based on difficulty of solving the discrete logarithm problem (DLP). Therefore, they claimed that their scheme is secure against various attacks. However, their scheme failed to preserve user anonymity, because in their scheme the user's real identity is transmitted over a public channel. Furthermore, He et al. [11] demonstrated that Wu et al.'s scheme [10] is vulnerable to privileged insider attacks. This attack is possible due to submission of user's chosen password in plaintext to the server in the registration phase. In addition, He et al. [11] proved that in the Wu et al.'s scheme [10], a legal user is able to impersonate other users. In order to overcome the weaknesses of Wu et al.'s scheme [10], He et al. proposed an improved DLP-based authentication scheme [11]. Their improved scheme [11] was more efficient than Wu et al.'s scheme [10], because it required less exponential operations. However, Wei et al. [12] demonstrated that both the Wu et al.'s scheme [10] and He et al.'s scheme [11] are insecure against off-line password guessing attacks. They showed that when an adversary steals or finds a smart card, he/she could guess the password of the owner of the smart card. To enhance the security, Wei et al. proposed another DLP-based authentication scheme [12]. Nevertheless, their improved scheme [12] does not provide user anonymity, because the user's real identity is transmitted through a public channel. Furthermore, Zhu [13] proved that the Wei et al.'s scheme [12] similar to the previous schemes is insecure against off-line password guessing attacks. Zhu [13] showed that an adversary who stolen a user's smart card and has eavesdropped the previous authentication messages, is able to guess the password of the owner of the smart card. To improve the security, Zhu [13] proposed an RSA-based authentication scheme. However, several studies [14–16] proved that Zhu's scheme [13] is insecure against password guessing attacks, impersonation attacks, parallel attacks, smart card lost attacks, and denial-of service attacks, and also does not provide key agreement and user anonymity.

All above mentioned authentication schemes are based on two factors. That is, in those schemes, the user to complete the authentication and key agreement process, must know a secret (e.g., password), and must have a token (e.g., smart card, mobile device, etc.). However, the secret can be guessed, shared, or disclosed, and the token may be stolen, lost, duplicated, or given to others. Therefore, to enhance the security, researchers introduced a new type of authentication, called three-factor authentication, which uses three factors for authentication. In this type of authentication, biometrics (e.g. iris, face, retina, fingerprint, etc.) are used as a third factor for authentication. Since biometrics cannot be guessed, forged, shared, duplicated, stolen, or given to others [17], by employment of biometrics, before mentioned problems could be eliminated.

Recently, Awasthi et al. [18] proposed a biometric-based authentication scheme for TMIS. Because of employing only hash and XOR operations for authentication and key agreement, their scheme was a lightweight and efficient authentication scheme. However, since the values of the user's identity and biometric are stored in plaintext on the smart card, if an adversary acquires the user's smart card, then he/she can guess the user's password in an off-line manner. Therefore, their scheme is vulnerable to password guessing attacks once the smart card is stolen [19]. In addition, in the password change phase of their scheme, the smart card only checks the inputted biometric and does not check the inputted old password. Therefore, if a user mistakenly enters a wrong old password, then he/she will no longer be able to pass the verification process of the smart card and login to the server [20]. Furthermore, Tan in [20] proved that Awasthi et al.'s scheme [18] is vulnerable to reflection attacks and does not provide user anonymity and three-factor security. To improve the security of the Awasthi et al.'s scheme [18], Tan in [20] proposed a biometric-based authentication scheme for TMIS using elliptic curve cryptosystem (ECC) [40]. Elliptic curve discrete logarithm problem (ECDLP) is considerably more difficult than the discrete logarithm problem (DLP) and the integer factorization problem (RSA is the well-known example) [41, 42]. Hence, the elliptic curve cryptosystems need a smaller key size than the other public-key cryptosystems to achieve a same security level (a 1,024-bit RSA key is equivalent to a 160-bit ECC key) [43, 44]. The higher speed and lower power consumption are the result of reduction in the key size [41, 45]. Therefore, the performance of the Tan's scheme [20] is better than the previous schemes in both efficiency and security. However, in this paper, we show that the Tan's enhanced authentication scheme [20] is insecure against replay attacks and denial-of-service attacks. Furthermore, in order to improve security and efficiency of the Tan's scheme [20], we propose a new ECC-based three-factor anonymous authentication and key agreement scheme for TMIS.

The rest of paper is organized as follows. Tan's scheme is reviewed in Section "Review of the Tan's scheme". Weaknesses of the Tan's scheme are discussed in Section "Weaknesses of the Tan's scheme". In Section "The proposed scheme", a new three-factor anonymous authentication and key agreement scheme for TMIS is proposed. Security and performance of the proposed scheme is analyzed in Sections "Security analysis" and "Performance analysis", respectively. Finally, the paper is concluded in Section "Conclusion".

Review of the Tan's scheme

In this section, we will briefly review Tan's authentication scheme for TMIS [20]. Tan's scheme consists of four phases as follows, namely registration phase, login phase, authentication and key agreement phase, and password and biometric update phase. The definition of notations used throughout this paper is summarized in Table 1.

Table 1 Definition of notations used in this paper

Symbol	Definition
B_i	The biometric template for i_{th} patient
N	A large prime number
E	An elliptic curve with order n
P	The base point of the elliptic curve E with order n
rP	The point multiplication defined as $rP = \underbrace{P+P+\cdots+P}_{r \text{ times}}$
x	The telecare server's secret key
Y	The telecare server's public key, $Y = xP$
PW_i	The password for i_{th} patient
MPW_i	The masked password of i_{th} patient
MB_i	The masked biometric template of i_{th} patient
MID_i	The masked identity of i_{th} patient
$d\,(.)$	A symmetric parametric function
τ	A threshold for biometric verification
$\|\|$	The concatenation operation
$\oplus$	The bit-wise exclusive-or (XOR)
N_C	A random number chosen by the patient
N_S	A random number chosen by the telecare server
SK	A shared session key between the patient and the telecare server
T_C / T_S	The current time of the patient's system/the telecare server
$\varDelta T$	The maximum transmission delay
AID_i	The authenticator for i_{th} patient

Registration phase

Before a user (e.g. patient, doctor, nurse, etc.) can use the telecare server's services, the user has to register with the telecare server. At the end of the registration phase that is performed once for each user, the user obtains a smart card that contains the required information for accessing the provided services.

Step 1: The patient chooses an identity ID_i, a password PW_i, and a random number N_C. Then, he/she imprints his/her biometric B_i at a sensor, computes $d = h(PW_i \oplus B_i) \oplus N_C$ and submits ID_i and d to the telecare server through a secure channel.

Step 2: Upon receiving ID_i and d, the telecare server computes $c = h(ID_i||x) \oplus d$, stores $\{c, P, h(\bullet), n, Y\}$ into a smart card and sends the smart card to the patient through the secure channel.

Step 3: When the patient receives the smart card, he/she computes $d_1 = c \oplus N_C$ and $d_2 = h(PW_i||B_i||ID_i)$, and replaces c with $\{d_1, d_2\}$ in his/her smart card.

Login phase

A registered patient can access the telecare server's information and services by successfully performing the login and authentication phases. In the login phase that is the first check point, the smart card checks the legitimacy of the patient by verifying the inputted identity, password, and biometric. In this phase, the patient inserts his/her smart card into a card reader, enters his/her ID_i and PW_i, and imprints his/her biometric B_i at the sensor. After that, the smart card computes $d_2^* = h(PW_i||B_i||ID_i)$ and checks whether d_2^* is equal to d_2 or not. If they are equal, the smart card chooses a random number $r_i \in_R Z_p^*$, and computes $R_1 = r_iP$, $R_2 = r_iY$, $v_i = ID_i \oplus h(R_1||R_2)$, $x_i = d_1 \oplus h(PW_i \oplus B_i)$, and $z_i = h(ID_i||v_i||R_1||R_2||x_i)$. Finally, the smart card sends the message (R_1, v_i, z_i) to the telecare server through a public channel.

Authentication and key agreement phase

This phase is initiated when the patient passes the verification process of the login phase. In this phase, the patient and the telecare server mutually authenticate each other to thwart security attacks. Furthermore, they negotiate a shared session key that will be used to encrypt/decrypt and authenticate subsequent communications. During this phase, the following steps are performed.

Step 1: Upon receiving the message (R_1, v_i, z_i), the telecare server computes $R_2^* = xR_1$, $ID_i^* = v_i \oplus h(R_1||R_2^*)$, $x_i^* = h(ID_i^*||x)$, and $z_i^* = h(ID_i^*||v_i||R_1||R_2^*||x_i^*)$, and checks whether

z_i^* is equal to the received z_i or not. If they are not equal, it halts the process. Otherwise, the telecare server authenticates the patient. After that, the telecare server chooses a random number $r \in_R Z_p^*$, computes $R = rP$ and $z = h(rR_1 \| R_2^* \| R \| x_i^*)$, and sends a message (R, z) to the patient through the public channel. Finally, it computes the session key SK as $SK = h(rR_1 \| ID_i^* \| R \| x_i^*)$.

Step 2: When the patient receives the message (R, z), he/she computes $z^* = h(r_iR \| R_2 \| R \| x_i)$ and checks whether z^* is equal to the received z or not. If they are equal, the telecare server is authenticated by the patient and the patient computes the session key SK as $SK = h(r_iR \| ID_i \| R \| x_i)$.

Password and biometric update phase

When a patient suspects that his/her password is used or misused by a third party, he/she must change the password immediately. When a patient wants to change his/her password and biometric, he/she inserts his/her smart card into the card reader and inputs his/her ID_i, PW_i, and B_i. Then, the smart card computes $d_2^* = h(PW_i \| B_i \| ID_i)$ and checks whether d_2^* is equal to d_2 or not. If they are equal, it asks the user to input a new password PW_i^{New} and a new biometric B_i^{New}. After entering PW_i^{New} and B_i^{New} by the patient, the smart card computes $d_1^{New} = d_1 \oplus h(PW_i \oplus B_i) \oplus h(PW_i^{New} \oplus B_i^{New})$, and $d_2^{New} = h(PW_i^{New} \| B_i^{New} \| ID_i)$, and replaces d_1 and d_2 with d_1^{New} and d_2^{New}, respectively.

Weaknesses of the Tan's scheme

In this section, we will show that Tan's scheme [20] is vulnerable to replay attacks and denial-of-service attacks.

Replay attacks

Suppose an adversary has eavesdropped a past login message (R_1, v_i, z_i). He/she is able to launch a replay attack and login to the telecare server by re-sending the eavesdropped message (R_1, v_i, z_i) to the telecare server. In other words, the adversary without running the "Login phase", sends the eavesdropped message (R_1, v_i, z_i) to the telecare server. In the "Authentication and key agreement phase", upon receiving the message (R_1, v_i, z_i), the telecare server computes $R_2^* = xR_1$, $ID_i^* = v_i \oplus h(R_1 \| R_2^*)$, $x_i^* = h(ID_i^* \| x)$, and $z_i^* = h(ID_i^* \| v_i \| R_1 \| R_2^* \| x_i^*)$, and checks whether z_i^* is equal to the received z_i or not. Since z_i and z_i^* are equal, the telecare server will authenticate the adversary, and the adversary will be able to login to the telecare server. Thus, the adversary can easily login to the telecare server by re-sending an old login message.

Since the telecare server does not check the freshness of the received login message (R_1, v_i, z_i), and authenticates the patient in Step 1 of the "Authentication and key agreement phase", the telecare server will not be able to discover replay attacks.

Denial-of-service attacks

Due to avalanche effect of hash functions that a change in an input bit can effect one half of output bits averagely [46], if a noisy data (e.g. biometrics) be considered as input of a hash function, the output of the hash function differs hugely for each input (same biometrics) [47].

In the registration phase of the Tan's scheme, the patient computes $d_2 = h(PW_i \| B_i \| ID_i)$ using his/her identity ID_i, password PW_i, and personal biometric B_i. Then, he/she stores d_2 in the smart card for the verification process in the login phase. In the login phase, the patient inserts his/her smart card into a card reader, enters his/her ID_i and PW_i, and imprints his/her biometric B_i^* at the sensor. The verification is performed by checking whether $d_2^* = h(PW_i \| B_i^* \| ID_i)$ is equal to stored d_2 or not. However, this verification may never pass because $d_2^* = d_2$ may never hold. Since the inputted biometrics of a same patient may vary in each time [48], the equation $d_2^* = d_2$ may never hold due to the avalanche property of the hash function. As a result, the legal patient may be unable to pass the verification process at the login phase. Therefore, Tan's scheme [20] is vulnerable to denial-of-service attacks.

The proposed scheme

In this section, we explain our proposed three-factor anonymous authentication and key agreement scheme for TMIS. The proposed scheme improves both the security and efficiency of the Tan's scheme. In the proposed scheme, in order to withstand the replay attack that is discussed in Subsection Replay attacks, we use a timestamp and two fresh random numbers to ensure the freshness of the login and authentication messages. Therefore, the server can check the freshness of the login message by verifying the timestamp and random numbers. Furthermore, in the proposed scheme the server authenticates the patient after receiving and verifying the corresponding response message from the patient in Step A3 of login and authentication phase. It should be noted that in the Tan's scheme [20], the server authenticates the patient after receiving and verifying the first login message, and also it does not check the freshness of the received login message. In order to solve the denial-of-service problem of the Tan's scheme that is discussed in Subsection Denial-of-service attacks, instead of using a hash function for biometric verification, we use a symmetric parametric function that determines differences between two biometric templates. In order to reduce the computational complexity, we use two 160-bit modular multiplications and one 160-bit modular inversion instead of two elliptic curve point multiplications in the Tan's scheme [20]. Since, the cost of an elliptic curve point multiplication is equivalent to the cost of 1,200 modular multiplications or 400 modular inversions [49], the computational cost is reduced significantly in comparison with the Tan's scheme. The proposed scheme consists of four phases: system setup phase, registration phase, login and authentication phase, and password and biometric update phase. Details of these phases are described in the following subsections.

System setup phase

In order to select and determine the security functions, parameters, and variables, which will be used by the server and users during the registration, login and authentication, and password and biometric update phases, the telecare server runs this phase once at the system initialization time. In this phase, the telecare server chooses an elliptic curve E [50], and selects a base point P with the large order n over E. Then, the telecare server selects a random integer $x \in_R Z_p^*$ as its secret key and computes its public key $Y = xP$. Furthermore, the telecare server selects two secure one-way hash functions $h(\bullet)$: $\{0,1\}^* \rightarrow \{0,1\}^s$, and $h_1(\bullet)$: $\{0,1\}^* \rightarrow Z_p^*$, where s is the output size. Finally, the telecare server publishes $(E, n, P, Y, h(\cdot), h_1(\cdot))$ as system parameters and keeps x securely.

Registration phase

Before a user (e.g. patient, doctor, nurse, etc.) can use the telecare server's services, the user has to register with the telecare server. At the end of the registration phase that is performed once for each user, the user obtains a smart card that contains the required information for accessing the provided services. As illustrated in Fig. 1, the registration process of the proposed scheme proceeds as follows.

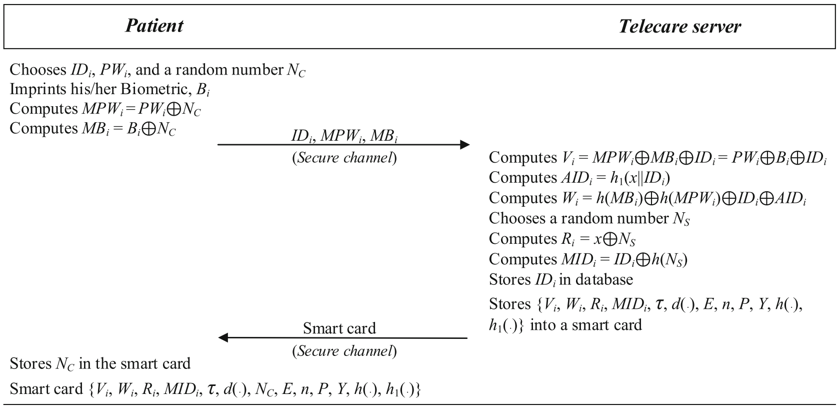
Step R1: The patient chooses an identity, ID_i, a password, PW_i, and a random number, N_C. Furthermore, he/she imprints his/her biometric B_i at a sensor. After that, he/she computes his/her masked password MPW_i as $MPW_i = PW_i \oplus N_C$ and his/her masked biometric MB_i as $MB_i = B_i \oplus N_C$. Finally, he/she sends ID_i, MPW_i, and MB_i to the telecare server through a secure channel.

Step R2: Upon receiving ID_i, MPW_i, and MB_i, the telecare server checks whether ID_i is already in database or not. If ID_i does not exist, the telecare server computes $AID_i = h_1(x||ID_i)$, $V_i = MPW_i \oplus MB_i \oplus ID_i = PW_i \oplus N_C \oplus B_i \oplus N_C \oplus ID_i = PW_i \oplus B_i \oplus ID_i$, and $W_i = h(MB_i) \oplus h(MPW_i) \oplus ID_i \oplus AID_i$. Furthermore, the telecare server selects a random number N_S and computes $R_i = x \oplus N_S$, and $MID_i = ID_i \oplus h(N_S)$. Then, the telecare server stores ID_i in its database and the information $\{V_i, W_i, R_i, MID_i, \tau, d(.), E, n, P, Y, h(.), h_1(.)\}$ into a smart card. Note that $d(.)$ is a function that determines differences between two biometric templates that are even if belong to a same person, may have a few differences, and τ is a threshold for acceptability of this difference [51]. Finally, the telecare server sends the smart card to the patient through the secure channel.

Step R3: When the patient receives the smart card, he/she stores the random number N_C in the memory of it.

Login and authentication phase

A registered patient can access the telecare server's information and services by successfully performing the login and authentication phase. In this phase, first the smart card checks the legitimacy of the patient by verifying the inputted identity, ID_i, password, PW_i, and biometric, B_i. Then, the patient and the telecare server mutually authenticate each other to thwart security attacks. Meanwhile, they negotiate a shared session key that will be used to encrypt/decrypt and authenticate



Chooses ID_i, PW_i, and a random number N_C
Imprints his/her Biometric, B_i
Computes $MPW_i = PW_i \oplus N_C$
Computes $MB_i = B_i \oplus N_C$

Computes $V_i = MPW_i \oplus MB_i \oplus ID_i = PW_i \oplus B_i \oplus ID_i$
Computes $AID_i = h_1(x||ID_i)$
Computes $W_i = h(MB_i) \oplus h(MPW_i) \oplus ID_i \oplus AID_i$
Chooses a random number N_S
Computes $R_i = x \oplus N_S$
Computes $MID_i = ID_i \oplus h(N_S)$
Stores ID_i in database
Stores $\{V_i, W_i, R_i, MID_i, \tau, d(.), E, n, P, Y, h(.), h_1(.)\}$ into a smart card

Stores N_C in the smart card
Smart card $\{V_i, W_i, R_i, MID_i, \tau, d(.), N_C, E, n, P, Y, h(.), h_1(.)\}$

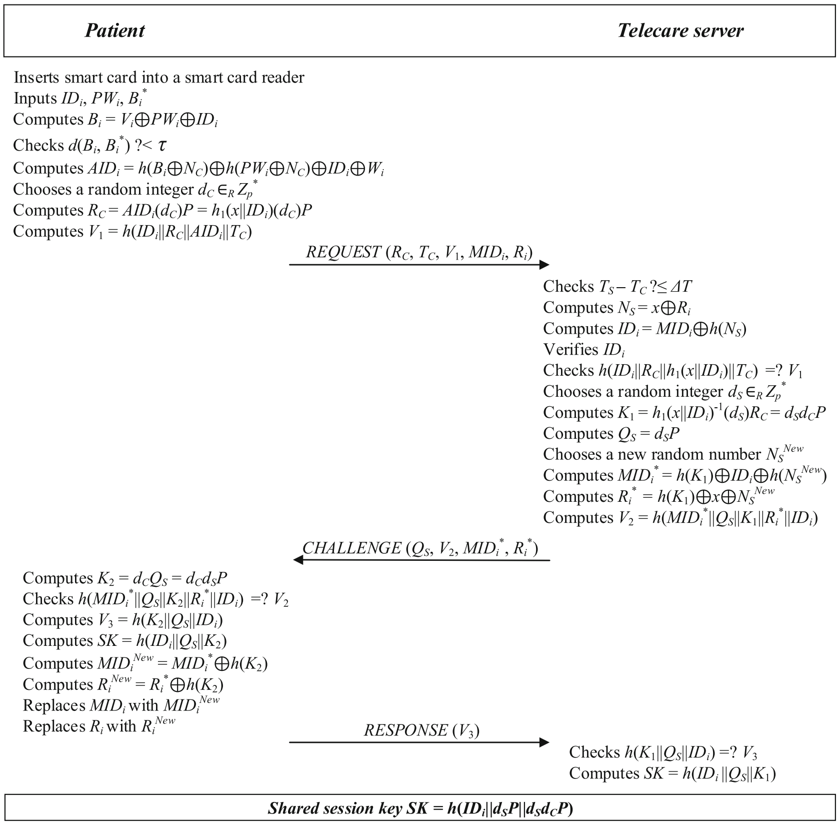
Fig. 1 Registration phase of the proposed scheme

subsequent communications. After the mutual authentication, the patient can login to the telecare server and obtain desired services. In this phase that is running frequently, the patient communicates with the telecare server through a public channel. As illustrated in Fig. 2, this phase includes the following steps.

Step A1: The patient inserts his/her smart card into a smart card reader, enters his/her ID_i, and PW_i, and imprints his/her biometric B_i^* at the sensor. Then, the smart card computes $B_i = V_i \oplus PW_i \oplus ID_i$ and checks whether the equation $d(B_i, B_i^*) < \tau$ holds or not. If the equation does not hold, it halts the process. Otherwise, it extracts the authenticator of the patient as $AID_i = h(B_i \oplus N_C) \oplus h(PW_i \oplus N_C) \oplus ID_i \oplus W_i$, chooses a random integer $d_C \in_R Z_p^*$, computes $R_C = AID_i(d_C)P = h_1(x\|ID_i)(d_C)P$, and $V_1 = h(ID_i\|R_C\|AID_i\|T_C)$, and sends a request message as *REQUEST* $(R_C, T_C, V_1, MID_i, R_i)$ to the telecare server. Note that T_C is the current time of the patient's system.

Step A2: Upon receiving the message *REQUEST* $(R_C, T_C, V_1, MID_i, R_i)$ at the time T_S, the telecare server checks whether the equation T_S - $T_C \leq \Delta T$ holds or not. If the equation does not hold, the telecare server rejects the *REQUEST* message. Otherwise, the telecare server computes $N_S = x \oplus R_i$, extracts ID_i as $ID_i = MID_i \oplus h(N_S)$, and checks whether ID_i is exist in database or not. If it does not exist, the telecare server terminates the session. Otherwise, it computes $h(ID_i\|R_C\|h_1(x\|ID_i)\|T_C)$, and checks whether it is equal to the received V_1 or not. If they are not equal, the telecare server terminates the session. Otherwise, the telecare server chooses a random integer $d_S \in_R Z_p^*$, and computes $Q_S = d_S P$ and $K_1 = h_1(x\|ID_i)^{-1}(d_S)R_C = h_1(x\|ID_i)^{-1}(d_S)$-$h_1(x\|ID_i)(d_C)P = d_S d_C P$. Furthermore, it selects a random number N_S^{New} and computes $R_i^* = h(K_1) \oplus x \oplus N_S^{New}$, $MID_i^* = h(K_1) \oplus ID_i \oplus h(N_S^{New})$, and $V_2 = h(MID_i^*\|Q_S\|K_1\|R_i^*\|ID_i)$. Finally, the telecare server sends the message *CHALLENGE* $(Q_S, V_2, MID_i^*, R_i^*)$ to the patient.

Step A3: After receiving the message *CHALLENGE* $(Q_S, V_2, MID_i^*, R_i^*)$, the patient computes $K_2 = d_C Q_S = d_C d_S P$ and checks whether $h(MID_i^*\|Q_S\|K_2\|R_i^*\|$-$ID_i)$ is equal to the received V_2 or not. If they are not equal, the patient stops the session. Otherwise, he/she authenticates the telecare server, and computes $MID_i^{New} = MID_i^* \oplus h(K_2)$, that is equal to $ID_i \oplus h(N_S^{New})$, and $R_i^{New} = R_i^* \oplus h(K_2)$, that is equal to $x \oplus N_S^{New}$. Then, the patient updates the values of MID_i and R_i that are stored in the smart



Patient ***Telecare server***

Inserts smart card into a smart card reader
Inputs ID_i, PW_i, B_i^*
Computes $B_i = V_i \oplus PW_i \oplus ID_i$
Checks $d(B_i, B_i^*)$?< τ
Computes $AID_i = h(B_i \oplus N_C) \oplus h(PW_i \oplus N_C) \oplus ID_i \oplus W_i$
Chooses a random integer $d_C \in_R Z_p^*$
Computes $R_C = AID_i(d_C)P = h_1(x\|ID_i)(d_C)P$
Computes $V_1 = h(ID_i\|R_C\|AID_i\|T_C)$

REQUEST $(R_C, T_C, V_1, MID_i, R_i)$

Checks $T_S - T_C$?≤ ΔT
Computes $N_S = x \oplus R_i$
Computes $ID_i = MID_i \oplus h(N_S)$
Verifies ID_i
Checks $h(ID_i\|R_C\|h_1(x\|ID_i)\|T_C)$ =? V_1
Chooses a random integer $d_S \in_R Z_p^*$
Computes $K_1 = h_1(x\|ID_i)^{-1}(d_S)R_C = d_S d_C P$
Computes $Q_S = d_S P$
Chooses a new random number N_S^{New}
Computes $MID_i^* = h(K_1) \oplus ID_i \oplus h(N_S^{New})$
Computes $R_i^* = h(K_1) \oplus x \oplus N_S^{New}$
Computes $V_2 = h(MID_i^*\|Q_S\|K_1\|R_i^*\|ID_i)$

CHALLENGE $(Q_S, V_2, MID_i^*, R_i^*)$

Computes $K_2 = d_C Q_S = d_C d_S P$
Checks $h(MID_i^*\|Q_S\|K_2\|R_i^*\|ID_i)$ =? V_2
Computes $V_3 = h(K_2\|Q_S\|ID_i)$
Computes $SK = h(ID_i\|Q_S\|K_2)$
Computes $MID_i^{New} = MID_i^* \oplus h(K_2)$
Computes $R_i^{New} = R_i^* \oplus h(K_2)$
Replaces MID_i with MID_i^{New}
Replaces R_i with R_i^{New}

RESPONSE (V_3)

Checks $h(K_1\|Q_S\|ID_i)$ =? V_3
Computes $SK = h(ID_i\|Q_S\|K_1)$

Shared session key $\boldsymbol{SK = h(ID_i\|d_S P\|d_S d_C P)}$

Fig. 2 Login and authentication phase of the proposed scheme

card with the values of MID_i^{New} and R_i^{New}, respectively. Finally, the patient computes $V_3 = h(K_2||Q_S||ID_i)$, and the shared session key SK as $SK = h(ID_i||Q_S||K_2)$, and sends a message *RESPONSE* (V_3) to the telecare server.

Step A4: Upon receiving the message *RESPONSE* (V_3), the telecare server checks whether $h(K_1||Q_S||ID_i)$ is equal to V_3 or not. If they are not equal, the telecare server ignores the *RESPONSE* message. Otherwise, the telecare server authenticates the patient and computes the shared session key SK as $SK = h(ID_i\ ||Q_S||K_1)$.

Password and biometric update phase

When a patient suspects that his/her password is used or misused by a third party, he/she must change the password immediately. In this phase, the patient can update his/her old password PW_i to a new password PW_i^{New} and his/her old biometric B_i to a new biometric B_i^{New}. This phase includes the following steps.

Step P1: The patient inserts his/her smart card into a smart card reader, enters his/her ID_i and PW_i and imprints his/her biometric B_i^* at the sensor.

Step P2: The smart card computes $B_i = V_i \oplus PW_i \oplus ID_i$ and checks whether the equation $d(B_i, B_i^*) < \tau$ holds or not. If the equation does not hold, the smart card halts the process. Otherwise, it shows a message to the patient that indicates "please input your new password and biometric".

Step P3: The patient enters a new password PW_i^{New} and imprints a new personal biometric B_i^{New}.

Step P4: The smart card computes V_i^{New} and W_i^{New} as follows.

$$\begin{aligned}
V_i^{New} &= PW_i^{New} \oplus B_i^{New} \oplus PW_i \oplus B_i \oplus V_i\\
&= PW_i^{New} \oplus B_i^{New} \oplus PW_i \oplus B_i \oplus PW_i \oplus B_i \oplus ID_i\\
&= PW_i^{New} \oplus B_i^{New} \oplus ID_i\\
W_i^{New} &= h\left(B_i^{New} \oplus N_C\right) \oplus h\left(PW_i^{New} \oplus N_C\right) \oplus h(B_i \oplus N_C) \oplus h(PW_i \oplus N_C) \oplus W_i\\
&= h\left(B_i^{New} \oplus N_C\right) \oplus h\left(PW_i^{New} \oplus N_C\right) \oplus h(B_i \oplus N_C) \oplus h(PW_i \oplus N_C) \oplus h(B_i \oplus N_C) \oplus h(PW_i \oplus N_C) \oplus ID_i \oplus AID_i\\
&= h\left(B_i^{New} \oplus N_C\right) \oplus h\left(PW_i^{New} \oplus N_C\right) \oplus ID_i \oplus AID_i
\end{aligned}$$

Finally, the smart card replaces V_i and W_i with V_i^{New} and W_i^{New}, respectively.

Security analysis

In this section, resistance of the proposed scheme against various security attacks such as impersonation attacks, replay attacks, denial-of-services attacks, stolen verifier attacks, password guessing attacks, privileged insider attacks, and modification attacks is examined. Furthermore, functionality of our proposed scheme to provide some security requirements, such as perfect forward secrecy, known-key security, and patient's anonymity is investigated.

Impersonation attacks

Suppose an adversary steals or finds a smart card and wants to impersonate a legal patient. Even if the adversary derives V_i, W_i, N_C, MID_i, and R_i from the smart card, he/she is not able to obtain the right value $h_1(x||ID_i)$ without knowing the values of PW_i, ID_i, and B_i. Thus, he/she cannot compute a valid request message as *REQUEST* $(R_C, T_C, V_1, MID_i, R_i)$, where $R_C = h_1(x||ID_i)(d_C)P$ and $V_1 = h(ID_i||R_C||h_1(x||ID_i)||T_C)$. Therefore, the adversary cannot impersonate a legal patient. On the other hand, suppose the adversary wants to impersonate a legal telecare server and spoof the patient, the adversary has to produce a valid data V_2 as $V_2 = h(MID_i^*||Q_S||K_1||R_i^*||ID_i)$. However, since the adversary does not know the telecare server's secret key, x, he/she cannot compute $K_1 = h_1(x||ID_i)^{-1}(d_S)R_C$, where $R_C = h_1(x||ID_i)(d_C)P$. Therefore, the adversary is not able to produce a valid challenge message and he/she cannot impersonate a legal telecare server.

Hence, the proposed scheme is secure against impersonation attacks and mutual authentication is provided in our scheme.

Replay attacks

As discussed in Subsection Replay attacks, the Tan's scheme [20] is vulnerable to replay attacks because the telecare server does not check the freshness of the received login message $\{R_1, v_i, z_i\}$, and also the telecare server authenticates the patient after receiving and verifying the first login message in Step 1 of the "Authentication and key agreement phase". In order to withstand replay attacks, we use a timestamp, T_C, and two fresh random numbers d_C and d_S to ensure the freshness of the login and authentication messages. Furthermore, in the proposed scheme, the telecare server authenticates the patient after receiving and verifying the message *RESPONSE* (V_3) in Step A3 of the login and authentication phase.

Suppose an adversary re-sends an old message *REQUEST* (R_C, T_C, V_1, MID_i, R_i) to the medical server. The telecare server can detect a replay attack by checking the condition T_S - T_C ? ≤ ΔT, where T_S and ΔT denotes the telecare server's current time and the maximum transmission delay, respectively. Note that, if the adversary changes the timestamp T_C in the request message, then the telecare server is able to detect this modification by checking V_1 = ? $h(ID_i \| R_C \| h_1(x \| ID_i) \| T_C^*)$, where T_C^* denotes the changed timestamp. Furthermore, even if the adversary immediately re-sends an eavesdropped *REQUEST* message to the telecare server and passes the freshness checking, he/she when receives the message *CHALLENGE* (Q_S, V_2, MID_i^*, R_i^*) in the Step A2 of the login and authentication phase, cannot generate a valid message *RESPONSE* (V_3). Since the adversary does not know the patient's identity ID_i and the random number d_C, he/she cannot compute a correct value V_3 as $V_3 = h(d_C Q_S \| Q_S \| ID_i)$. Therefore, our proposed scheme is secure against replay attacks.

Denial-of-service attacks

In the Tan's scheme, a hash function is used to check the validity of the inputted biometric, password and identity. As discussed in the Subsection Denial-of-service attacks, due to the avalanche property of hash functions and the noise feature of biometrics, a legal patient may never pass the verification process at the login phase. In order to solve this problem, we use a symmetric parametric function d (.) that determines differences between two biometric templates [51]. In the proposed scheme, the patient's biometric template B_i is stored in the memory of the smart card in a protected manner. When the patient wants to login to the server, he/she inserts his/her smart card in the card reader and keys in his/her identity ID_i and password PW_i, and imprints his/her biometric B_i^* at the sensor. Then, the smart card extracts the stored biometric B_i as $B_i = V_i \oplus PW_i \oplus ID_i$ and checks whether the equation $d(B_i, B_i^*) < \tau$ holds or not. If the equation holds, the patient will pass the verification process. In [51] it is demonstrated that the inputted biometric B_i^* with some differences with the stored biometric template B_i (the difference between them must be less than the predetermined threshold τ) could pass the biometric verification process. Therefore, the proposed scheme is immune from denial-of service attacks.

Stolen verifier attacks

In the proposed scheme, the telecare server does not maintain any passwords, biometrics or verification information of patients in its database. Therefore, even if an adversary accesses the database of the telecare server, he/she still is not able to find the authentication information of the patients.

Password guessing attacks

Suppose an adversary steals or finds a smart card and extracts the information {V_i, W_i, N_C, R_i, MID_i} that are stored in the smart card, where $W_i = h(B_i \oplus N_C) \oplus h(PW_i \oplus N_C) \oplus ID_i \oplus h_1(x \| ID_i)$, $V_i = PW_i \oplus B_i \oplus ID_i$, $R_i = x \oplus N_S$, and $MID_i = ID_i \oplus h(N_S)$. However, since the adversary has no knowledge of the telecare server's secret key x, the patient's biometric template B_i, and the patient's identity ID_i, he/she is not able to obtain the patient's password PW_i. Even if the adversary has recorded all the previous authentication messages, he/she still is not able to relate the stolen smart card with its corresponding authentication messages to guess a correct password and identity. Because the patient's identity is not stored in plaintext on the smart card as well as it is not sent in plaintext in the authentication messages. Therefore, the proposed scheme is secure against off-line password guessing attacks. In addition, online password guessing attacks can be defeated by limiting the number of failed login requests.

Privileged insider attacks

In the proposed scheme, the patient in order to register himself/herself in a telecare server, submits his/her masked password $MPW_i = PW_i \oplus N_C$, and his/her masked biometric $MB_i = B_i \oplus N_C$, where N_C is a random number. Since the privileged staff at the server side does not know the random number N_C, he/she is not able to retrieve patient's password PW_i, or the patient's biometric B_i. Therefore, the proposed scheme is immune from privileged insider attacks.

Modification attacks

In the proposed scheme, authentication messages include the verification data V_1, V_2, and V_3. The verification data V_1 is generated by a hash function using secret values ID_i and $h_1(x \| ID_i)$. Both verification data V_2 and V_3 are produced by a hash function using ID_i and $K_1 = K_2 = d_C d_S P$. Since the adversary does not know ID_i, x and $d_C d_S P$, he/she cannot compute a right verification data as V_1, V_2, or V_3. Therefore, our proposed scheme is secure against modification attacks.

Perfect forward secrecy

In the proposed scheme, $SK = h(ID_i||d_SP||d_Sd_CP)$ is a shared session key between the patient and the telecare server. Even if an adversary obtains the telecare server's secret key, x, or the patient's password, PW_i, he/she cannot compute previous session keys, because without knowing d_C or d_S, it is difficult to compute d_Cd_SP. Besides, due to hardness of ECDLP [40], the adversary is not able to derive d_C from $R_C = h_1(x||ID_i)(d_C)P$, and d_S from $Q_S = d_SP$. Therefore, perfect forward secrecy is supported in our proposed scheme.

Known-key security

In the proposed scheme, the shared session key $SK = h(ID_i||d_SP||d_Sd_CP)$ changes in each session run. Even if an adversary somehow obtains a shared session key, he/she still is not able to compute other session keys. Because, values of d_C and d_S differ in each session run, and without knowing d_C or d_S, it is difficult to compute d_Cd_SP. Therefore, known-key security is provided in our proposed scheme.

Patient's anonymity

In our proposed scheme, the real identity of the patient is protected by a random number, N_S, that is chosen by the server as $MID_i = ID_i \oplus h(N_S)$. Since the adversary has no knowledge of the random number N_S, he/she is not able to obtain the real identity of the patient. In addition, an illegal server without knowing the secret key x, is not able to retrieve N_S from $R_i = x \oplus N_S$, therefore it cannot retrieve the patient's identity ID_i from $MID_i = ID_i \oplus h(N_S)$.

Functionality comparisons

In order to evaluate the functionality of the proposed scheme, we compare it with Tan's scheme [20] and some related schemes [14, 15, 21] in terms of security properties as summarized in Table 2. Xu et al.'s scheme [21] and Lee et al.'s scheme [15] are vulnerable to denial-of-service attacks, because in the password change phase of these schemes, the smart card does not verify the inputted old password [22]. Therefore, if a user during the password change process mistakenly enters a wrong old password, then he/she will no longer be able to pass the verification process of the smart card and login to the server. Tan's scheme [20] is vulnerable to replay attacks and denial-of-service attacks as demonstrated in Section "Weaknesses of the Tan's scheme". Khan et al.'s scheme [14] does not provide user anonymity as the real identity of the user is transmitted through a public channel. Furthermore, since the uniqueness of the user's identity is not checked in the registration process of the Khan et al.'s scheme, an adversary can register with an identity that corresponds to an existing user. When the adversary registers with an existing identity, he/she acquires a new smart card that has the same content with the victim's smart card. The adversary with the acquired smart card can easily impersonate the victim user. Therefore, Khan et al.'s scheme [14] is vulnerable to impersonation attacks. Lee et al.'s scheme [15] is vulnerable to replay attacks as stated in [22]. It is visible from the Table 2 that the proposed scheme is superior compared with other schemes.

Performance analysis

In this section, the performance of our proposed scheme is analyzed. Furthermore, the computation cost of the proposed scheme is compared with the Tan's scheme [20] and some related schemes [14, 15, 21].

In order to provide a precise computation cost comparison, we use the experiment data reported in [21] to evaluate schemes. Most recently, Xu et al. [21] evaluated the running time of the elliptic curve point multiplication and modular exponentiation operations by using C++ in the environment (CPU: 1.6 GHz, RAM: 2.0 GB). They reported that the average time of executing a modular exponentiation and a point multiplication is 1,910, and 1.49 ms, respectively. They also demonstrated that execution times of the hash function operation and exclusive-or operation (XOR) are negligible. Furthermore, Koblitz et al. [49] showed that the cost of executing an elliptic curve point multiplication is equivalent to the cost of 1,200 modular multiplications or 400 modular inversions. Therefore, we can conclude that execution of a 160-bit modular multiplication and a 160-bit modular inversion takes 0.00125 and 0.003725 ms, respectively.

For convenience, let T_{EXP}, T_{PM}, T_M, T_{INV}, T_X, and T_H denote the time complexity of executing a modular exponentiation, an elliptic curve point multiplication, a 160-bit modular multiplication, a 160-bit modular inversion, a bit-wise exclusive-or (XOR) operation and a one-way hash function operation, respectively. In order to evaluate the computation efficiency of different schemes, we use the simple method from [52]. For example, in the proposed scheme, four hash function operations and nine exclusive-or operations are needed to register a new user, therefore, the computational cost of the registration phase of our scheme is $4T_H + 9T_X$. In the login and authentication phase, four elliptic curve point multiplications, two 160-bit modular multiplications, one 160-bit modular inversion, 15 hash function operations, and 15 exclusive-or operations are required to accomplish mutual authentication and session key establishment. Therefore, the computational cost of the login and authentication phase of the proposed scheme is $4T_{PM} + 2T_M + 1T_{INV} + 15T_H + 15T_X$. Besides, four hash function operations and 14 exclusive-or operations are

Table 2 Security properties comparison

Security properties	Schemes				
	Ours	Tan [20]	Xu et al. [21]	Khan et al. [14]	Lee et al. [15]
Resist replay attacks	Yes	No	Yes	Yes	No
Resist impersonation attacks	Yes	Yes	Yes	No	Yes
Resist denial-of-service attacks	Yes	No	No	Yes	No
Resist password guessing attacks	Yes	Yes	Yes	Yes	Yes
Resist man-in-the-middle attacks	Yes	Yes	Yes	Yes	Yes
Resist stolen verifier attacks	Yes	Yes	Yes	Yes	Yes
Resist privileged insider attacks	Yes	Yes	Yes	Yes	Yes
Resist modification attacks	Yes	Yes	Yes	Yes	Yes
Provide user anonymity	Yes	Yes	Yes	No	Yes
Provide know-key security	Yes	Yes	Yes	Yes	Yes

required to update the password and biometric, therefore, the computational cost of the password and biometric update phase is $4T_H + 14T_X$. As a result, the total computational cost of our proposed scheme is $4T_{PM} + 2T_M + 1T_{INV} + 23T_H + 38T_X$, and the resulting computation time is (4*(1.49) + 2*(0.00125) + 0.003725) ≈ 5.97 ms.

The computational cost of the proposed scheme and related schemes [14, 15, 20, 21] during the registration, login and authentication, and password and biometric update processes are compared in Table 3. Khan et al.'s scheme [14] is a DLP-based authentication and key agreement scheme, which requires some exponential operations. Since the exponentiation is a time consuming operation, their scheme has computation overhead and is not suitable for medical networks involving resource constrained mobile devices. Moreover, Khan et al.'s scheme [14] does not provide user anonymity and is vulnerable to user impersonation attacks. Lee et al.'s scheme [15] is an RSA-based scheme, which requires two exponentiations to complete the mutual authentication and key agreement process. However, Lee et al.'s scheme [15] improved the performance by eliminating four exponentiations, but the computational cost is still high. Furthermore, Lee et al.'s scheme [15] is vulnerable to denial-of-services attacks and replay attacks [22]. Xu et al.'s scheme [21], Tan's scheme [20], and our proposed scheme rely on the ECDLP. Since the elliptic curve point multiplication is the basic and the main operation in elliptic curve cryptosystems and the time complexity of it, is lower than the time complexity of modular exponentiation ($1T_{EXP} \approx 8.2T_{PM}$ [49]), the computational cost is significantly reduced in these schemes. Tan's scheme [20] is vulnerable to replay attacks and both the Tan's scheme [20] and Xu et al.'s scheme [21] are vulnerable to denial-of-services attacks. Therefore, both the Xu et al.'s scheme [21], and Tan's scheme [20] are not suitable for TMIS. Table 3 shows that our improved scheme is more efficient than both the Xu et al.'s scheme [21] and the Tan's scheme [20]. In our scheme, two elliptic curve point multiplications are replaced with two 160-bit modular multiplications and one 160-bit modular inversion. Since, the modular multiplication and modular inversion has lower computation costs than the elliptic curve point multiplication ($1T_{PM} \approx 1200T_M \approx 400T_{INV}$ [49]), the total computation cost is reduced and efficiency is improved. As a result, we can conclude that our improved scheme is more efficient than other schemes.

Conclusion

In this paper, we have discovered two security weaknesses in the Tan's authentication scheme for telecare medicine

Table 3 Performance comparisons

Phases	Schemes				
	Ours	Tan [20] (2014)	Xu et al. [21] (2014)	Lee et al. [15] (2013)	Khan et al. [14] (2013)
Registration	$4T_H + 9T_X$	$3T_H + 4T_X$	$2T_H + 2T_X$	$2T_H + 1T_X$	$1T_{EXP} + 4T_H$
Login and authentication	$4T_{PM} + 2T_M + 1T_{INV} + 15T_H + 15T_X$	$6T_{PM} + 11T_H + 1T_X$	$6T_{PM} + 12T_H + 4T_X$	$2T_{EXP} + 10T_H + 4T_X$	$5T_{EXP} + 10T_H$
Password change	$4T_H + 14T_X$	$4T_H + 4T_X$	$2T_H + 2T_X$	$2T_H + 2T_X$	$6T_H$
Total cost	$4T_{PM} + 2T_M + 1T_{INV} + 23T_H + 38T_X$	$6T_{PM} + 18T_H + 9T_X$	$6T_{PM} + 16T_H + 8T_X$	$2T_{EXP} + 14T_H + 7T_X$	$6T_{EXP} + 20T_H$
Time	5.97 ms	8.94 ms	8.94 ms	3,820 ms	11,460 ms

information systems (TMISs). We have shown that Tan's scheme is vulnerable to replay attacks and denial-of-service attacks. In order to improve the security and efficiency, we have proposed a new anonymous three-factor ECC-based authentication and key agreement scheme for TMIS. According to the security and performance analysis, the proposed scheme not only withstands various attacks but it also is more efficient than Tan's scheme. Due to the better performance of the proposed scheme, our scheme is more suitable for TMIS.

References

1. Wen, F., Guo D., An improved anonymous authentication scheme for telecare medical information systems. *J. Med. Syst*. 38(5):1–11, 2014. doi:10.1007/s10916-014-0026-0.
2. Chen, H. M., Lo, J. W., Yeh, C. K., An efficient and secure dynamic ID-based authentication scheme for telecare medical information systems. *J. Med. Syst.* 36(6):3907–3915, 2012.
3. Nikooghadam, M., Zakerolhosseini, A., Secure communication of medical information using mobile agents. *J. Med. Syst.* 36(6):3839–3850, 2012.
4. Kim, K.-W., Lee, J.-D., On the security of two remote user authentication schemes for telecare medical information systems. *J. Med. Syst.* 2014. doi:10.1007/s10916-014-0017-1.
5. Wang, Y.-Y., Liu, J.-Y., Xiao, F.-X., Dan, J., A more efficient and secure dynamic ID-based remote user authentication scheme. *Comput. Commun.* 32(4):583–585, 2009.
6. Khan, M. K., Kim, S.-K., Alghathbar, K., Cryptanalysis and security enhancement of a more efficient & secure dynamic ID-based remote user authentication scheme. *Comput. Commun.* 34(3):305–309, 2011.
7. Xie, Q., Zhang, J., Dong, N., Robust anonymous authentication scheme for telecare medical information systems. *J. Med. Syst.* 2013. doi:10.1007/s10916-012-9911-6.
8. Jiang, Q., Ma, J.F., Ma, Z., Li, G.S., A privacy enhanced authentication scheme for telecare medical information systems. *J. Med. Syst.* 2013. doi:10.1007/s10916-012-9897-0.
9. Wu, F., Xu, L.L., Security analysis and improvement of a privacy authentication scheme for telecare medical information systems. *J. Med. Syst.* 2013. doi:10.1007/s10916-013-9958-z.
10. Wu, Z.Y., Lee, Y.C., Lai, F., Lee, H.C., Chung, Y., A secure authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(3):1529–1535, 2012.
11. He, D., Chen, J., Zhang, R., A more secure authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(3):1989–1995, 2012.
12. Wei, J., Hu, X., Liu, W., An improved authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(6):3597–3604, 2012.
13. Zhu, Z., An efficient authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(6):3833–3838, 2012.
14. Khan, M.K., Kumari, S., An authentication scheme for secure access to healthcare services. *J. Med. Syst.* 2013. doi:10.1007/s10916-013-9954-3.
15. Lee, T.-F., Liu, C.-M., A secure smart-card based authentication and key agreement scheme for telecare medicine information systems. *J. Med. Syst.* 2013. doi:10.1007/s10916-013-9933-8.
16. Muhaya, F. T. B., Cryptanalysis and security enhancement of Zhu's authentication scheme for telecare medicine information system. *Secur. Commun. Netw.* 2014. doi:10.1002/sec.967.
17. Radha, N., Karthikeyan, S., A study on biometric template security. ICTACT J Soft Comput 1(1):37–41, 2010.
18. Awasthi, A. K., Srivastava, K., A biometric authentication scheme for telecare medicine information systems with nonce. *J. Med. Syst.* 2013. doi:10.1007/s10916-013-9964-1.
19. Mishra, D., Mukhopadhyay, S., Kumari, S., Khan, M.K., Chaturvedi, A., Security enhancement of a biometric based authentication scheme for telecare medicine information systems with nonce. *J. Med. Syst.* 2014. doi:10.1007/s10916-014-0041-1.
20. Tan, Z., A user anonymity preserving three-factor authentication scheme for telecare medicine information systems. *J. Med. Syst.* 2014. doi:10.1007/s10916-014-0016-2.
21. Xu, X., Zhu, P., Wen, Q., Jin, Z., Zhang, H., He, L., A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems. *J. Med. Syst.* 2014. doi:10.1007/s10916-013-9994-8.
22. Das, A. K., Bruhadeshwar, B., An improved and effective secure password-based authentication and key agreement scheme using smart cards for the telecare medicine information system. *J. Med. Syst.* 37, 2013. doi:10.1007/s10916-013-9969-9.
23. Wu, Z.-Y., Chung, Y., Lai, F., Chen, T.-S., A password-based user authentication scheme for the integrated EPR information system. *J. Med. Syst.* 36(2):631–638, 2012. doi:10.1007/s10916-010-9527-7.
24. Hsiao, T.-C., Liao, Y.-T., Huang, J.-Y., Chen, T.-Z., Horng, G.-B., An Authentication Scheme to Healthcare Security under Wireless Sensor Networks. *J. Med. Syst.* 36(2):3649–3664, 2012. doi:10.1007/s10916-012-9839-x.
25. Yan, X., Li, W., Li, P., Wang, J., Hao, X., Gong, P., A Secure Biometrics-based Authentication Scheme for Telecare Medicine Information Systems. *J. Med. Syst.* 37, 2013. doi:10.1007/s10916-013-9972-1.
26. Cao, T., Zhai, J., Improved Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems .*J. Med. Syst.* 37, 2013. doi:10.1007/s10916-012-9912-5.
27. Lin, H.-Y., On the Security of A Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems. *J. Med. Syst.* 37, 2013. doi:10.1007/s10916-013-9929-4.
28. Hao, X., Wang, J., Yang, Q., Yan, X., and Li, P., A chaotic map-based authentication scheme for telecare medicine information systems. *J. Med. Syst.* 37:9919, 2013. doi:10.1007/s10916-012-9919-y.
29. Yau, W.-C., Phan, R. C.-W., Security Analysis of a Chaotic Map-based Authentication Scheme for Telecare Medicine Information Systems. *J. Med. Syst.* 37:9993, 2013. doi:10.1007/s10916-013-9993-9.
30. Chang, Y.-F., Yu, S.-H., Shiao, D.-R., An uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care. *J. Med. Syst.* 37:9902, 2013. doi:10.1007/s10916-012-9902-7.
31. Das, A. K., Goswami, A., A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care. *J. Med. Syst.* 37:9948, 2013. doi:10.1007/s10916-013-9948-1.
32. Wen, F., A robust uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care. *J. Med. Syst.* 37:9980, 2013. doi:10.1007/s10916-013-9980-1.
33. Zhao, Z., An Efficient Anonymous Authentication Scheme for Wireless Body Area Networks Using Elliptic Curve Cryptosystem. *J. Med. Syst.* 38, 2014. doi:10.1007/s10916-014-0013-5.
34. Mishra, D., Mukhopadhyay, S., Chaturvedi, A., Kumari, S., Khan, M. K., Cryptanalysis and Improvement of Yan et al.'s Biometric-Based Authentication Scheme for Telecare Medicine Information Systems. *J. Med. Syst.* 38, 2014. doi:10.1007/s10916-014-0024-2.
35. Das, A. K., Goswami, A., An Enhanced Biometric Authentication Scheme for Telecare Medicine Information Systems with Nonce Using Chaotic Hash Function. *J. Med. Syst.* 38, 2014. doi:10.1007/s10916-014-0027-z.
36. Xie, Q., Liu, W., Wang, S., Han, L., Hu, B., Wu, T., Improvement of a Uniqueness-and-Anonymity-Preserving User Authentication

Scheme for Connected Health Care. *J. Med. Syst.* 38, 2014. doi:10.1007/s10916-014-0091-4.

37. Jiang, Q., Ma, J., Lu, X., Tian, Y., Robust Chaotic Map-based Authentication and Key Agreement Scheme with Strong Anonymity for Telecare Medicine Information Systems. *J. Med. Syst.* 38, 2014. doi:10.1007/s10916-014-0012-6.
38. Li, C.-T., Lee, C.-C., Weng, C.-Y., A Secure Chaotic Maps and Smart Cards Based Password Authentication and Key Agreement Scheme with User Anonymity for Telecare Medicine Information Systems. *J. Med. Syst.* 38, 2014. doi:10.1007/s10916-014-0077-2.
39. Wen, F., A more secure anonymous user authentication scheme for the integrated EPR information system. *J. Med. Syst.* 2014. doi:10.1007/s10916-014-0042-0.
40. Hankerson, D., Menezes, A., Vanstone, S., *Guide to elliptic curve cryptography*. Springer, New York, USA, 2004.
41. Vanstone, S. A., Elliptic curve cryptosystem-the answer to strong, fast public-key cryptography for securing constrained environments. *Inf. Secur. Tech. Rep.* 12:78–87, 1997.
42. Nikooghadam, M., Zakerolhosseini, A., An efficient blind signature scheme based on the elliptic curve discrete logarithm problem. *The ISC International Journal of Information Security.* 8(10):125–131, 2009.
43. Stallings, W., *Cryptography and Network Security: Principles and Practice*, 4th edition. Prentice Hall, Upper Saddle River, NJ, 2005.
44. Zakerolhosseini, A., Nikooghadam, M., Secure Transmission of Mobile Agent in Dynamic Distributed Environments. *Wireless Personal Communications*, 70(2):641–656, 2013. doi:10.1007/s11277-012-0712-5.
45. Nikooghadam, M., Zakerolhosseini, A., Moghaddam, M.E., Efficient utilization of elliptic curve cryptosystem for hierarchical access control. *J. Syst. Softw.* 83(10):1917–1929, 2010.
46. Agarwal, S., Rungta, A., Padmavathy, R., Shankar, M., Rajan, N., An Improved Fast and Secure Hash Algorithm. *Journal of Information Processing Systems*. 8(1):119–132, 2012.
47. Linnartz, J.-P., Tuyls, P., New shielding functions to enhance privacy and prevent misuse of biometric templates. In: *Proceedings of the Audio- and Video-Based Person Authentication*. 2688:393–402, 2003. Guildford, UK. doi:10.1007/3-540-44887-X_47.
48. Nanavati, S., Thieme, M., Nanavati, R., *Biometrics: Identity Verification in a Networked World*. John Wiley & Sons, Inc., New York, NY, USA. 2002.
49. Koblitz, N., Menezes, A., Vanstone, S., The state of elliptic curve cryptography. *Des. Code. Crypt.* 19:173–193, 2000.
50. Johnson, D., Menezes, A., Vanstone, S., The elliptic curve digital signature algorithm (ECDSA). *Inter. J. Inf. Secur.* 1(1):36–63, 2001. doi:10.1007/s102070100002.
51. Inuma, M., Otsuka, A., Imai, H., Theoretical framework for constructing matching algorithms in biometric authentication systems. In: *Proc of ICB'09*. Lecture notes in computer science. 5558:806–815, 2009. Springer Berlin Heidelberg. doi:10.1007/978-3-642-01793-3_82.
52. He D., Chen J., Hu J., An ID-based client authentication with key agreement protocol for mobile client–server environment on ECC with provable security. Inf. Fusion 13(3):223–230, 2012.