J Med Syst (2015) 39: 32
DOI 10.1007/s10916-015-0221-7

An Enhanced Biometric-Based Authentication Scheme for Telecare Medicine Information Systems Using Elliptic Curve Cryptosystem

Yanrong Lu · Lixiang Li · Haipeng Peng · Yixian Yang

Received: 24 December 2014 / Accepted: 26 January 2015 / Published online: 14 February 2015

Abstract The telecare medical information systems (TMISs) enable patients to conveniently enjoy telecare services at home. The protection of patient's privacy is a key issue due to the openness of communication environment. Authentication as a typical approach is adopted to guarantee confidential and authorized interaction between the patient and remote server. In order to achieve the goals, numerous remote authentication schemes based on cryptography have been presented. Recently, Arshad et al.(J Med Syst 38(12): 2014) presented a secure and efficient three-factor authenticated key exchange scheme to remedy the weaknesses of Tan et al.'s scheme (J Med Syst 38(3): 2014). In this paper, we found that once a successful off-line password attack that results in an adversary could impersonate any user of the system in Arshad et al.'s scheme. In order to thwart these security attacks, an enhanced biometric and smart card based remote authentication scheme for TMISs is proposed. In addition, the BAN logic is applied to demonstrate the completeness of the enhanced scheme. Security and performance analyses show that our enhanced scheme satisfies more security properties and less computational cost compared with previously proposed schemes.

Keywords Authentication · Elliptic curve cryptosystem · Smart card · Biometric · Telecare medicine information systems

Introduction

With comprehensive employment of the mobile networks, TMISs enable telecare which builds a convenient bridge between patients at home and the remote server a reality. In such system, patients without leaving home can access the same medical services as at hospital. TMISs provide greatly facilitate for some patients who are inconvenient to go to hospital, which saves a lot of the patients' expenses and time. The problem is that the patients' sensitive information may be eavesdropped by an illegal entity due to the unreliable communication channel. Therefore, a feasible authentication mechanism [1–5] is essential needed to ensure security and integrity of transmitting data for TMISs.

In 2009, Wu et al. [6] presented an authenticated key exchange scheme for TMISs and declared their scheme was more efficient compared with the previous schemes for TMISs by adding a precomputation step. However, He et al.[7] identified that the scheme was susceptible to internal and masquerade attacks. Then, He et al. introduced a more secure authentication scheme to conquer these flaws. Later, Wei et al.[8] pointed out that both Wu et al. and He et al.'s schemes were prone to suffer from off-line password guessing attack. An improved scheme with more security

This article is part of the Topical Collection on *Mobile Systems*

Y. Lu · L. Li (✉) · H. Peng · Y. Yang
Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China
e-mail: li_lixiang2006@163.com

Y. Lu · L. Li · H. Peng · Y. Yang
National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing, 100876, China

was designed by Wei et al. But Zhu et al. [9] discovered that Wei et al.'s scheme was still insecure against off-line password guessing attack. In order to eliminate such pitfall, Zhu et al. further proposed an enhancement based on Wei et al.'s scheme using RSA [10]. In 2013, Wu et al. [11] pointed out that Jiang et al.'s scheme [12] had some security drawbacks and proposed a new authentication scheme for TMIS. Unfortunately, Wen et al. [13] observed that Wu et al.'s scheme did not provide patient anonymity and failed to resist server spoofing and off-line password guessing attacks. In order to erase these drawbacks, Wen et al. proposed their modified scheme based on Wu et al.'s scheme. Lately, other researchers also proposed their authentication and key agreement schemes for TMISs [14–16]. All in all, above schemes aim to achieve two factor authentication.

Lately, research in two factor based authenticated key exchange schemes employing biometric have attracted a lot of well-deserved attention. In comparison to password, biometrics keys have many advantages [17], such as cannot be lost or forgotten, copied or shared, hard to be forged or distributed and cannot be guessed easily. Many biometric based authentication schemes combine password and smart card were appeared [18–23], and were becoming one of the most widely adopted authentication mechanisms. Awasthi et al. [24] presented a biometric authentication nonce based scheme for TMISs. However, Mishra et al.[25] observed that Awasthi et al.'s scheme was vulnerable to off-line password guessing attack and did not provide efficient password change option. Soon after that Tan et al.[26] found that Awasthi et al.'s scheme did not resist reflection attack and did not achieve three factor security and user anonymity. To remedy the weaknesses of Awasthi et al.'s scheme, Tan et al. presented a three factor authentication scheme and claimed that their scheme was secure against various attacks. Recently, Arshad et al.[27] pointed out that Tan et al.'s scheme did not withstand denial-of service and replay attacks. They then presented an improved elliptic curve cryptosystem (ECC)-based [28, 29] scheme to prevent the flaws.

In this paper, we briefly review Arshad et al.'s scheme. We demonstrate Arshad et al.'s scheme fails to protect against off-line password guessing attack. Additionally, we show that in case the adversary succeeded in getting identity and password of an arbitrary user, he can impersonate any user of the system. Furthermore, we put forward a biometric based authentication scheme for TMISs to cope with the loopholes of Arshad et al.'s scheme. The proposed scheme also employs lower computational operations such as ECC and hash function to lower its computational cost. Besides, we adopt BAN logic [30] to demonstrate the completeness of the enhanced scheme. Moreover, we present the security and performance analyses to show that our enhanced scheme satisfies more security properties and less computational cost compared with previously proposed schemes.

The rest of this paper is organized as follows. Section "Review of Arshad et al.'s scheme" and Section "Weaknesses of Arshad et al.'s scheme"review and security analysis of Arshad et al.'s scheme, respectively. Section "Proposed scheme" and Section "Analysis security" show our proposed scheme and analyze its security. Section "Functionality and performance comparisons" depicts the functionality and performance comparison among the proposed scheme and other related ones. Section "Conclusion" is a brief conclusion.

Review of Arshad et al.'s scheme

This section briefly reviews Arshad et al.'s biometric based password authentication scheme for TMISs. Their scheme contains three phases: registration, authentication and password change. Notations that will be used throughout the paper are listed in Table 1.

Registration

(1) U selects his identity ID_i, password PW_i, a random number N_C and imprints his biometric B_i. Then, he computes $MPW_i = PW_i \oplus N_C$, $MB_i = B_i \oplus N_C$ and submits $\{ID_i, MPW_i, MB_i\}$ to S.

(2) S verifies whether ID_i is in his database or not. If ID_i is not found, S calculates $AID_i = h_2(x||ID_i)$, $V_i = MPW_i \oplus MB_i \oplus ID_i = PW_i \oplus B_i \oplus ID_i$, and $W_i = h_1(MB_i) \oplus h_1(MPW_i) \oplus ID_i \oplus AID_i$. Furthermore, S chooses a random number N_S and computes $R_i = x \oplus N_S$, and $MID_i = ID_i \oplus h_1(N_S)$. After that, S keeps ID_i in his database and the information $\{V_i, W_i, R_i, MID_i, \tau, d(\cdot), E, n, P, Y, h_1(\cdot), h_2(\cdot)\}$ into a smart card SC_i.

(3) U stores N_C into SC_i. Now, SC_i contains $\{N_C, V_i, W_i, R_i, MID_i, \tau, d(\cdot), E, n, P, Y, h_1(\cdot), h_2(\cdot)\}$

Table 1 Notations

$U,\ S$	The patient and the telecare server
$ID_i,\ PW_i,\ B_i$	Identity, password, biometric of the patient
$H(\cdot)$	Biohash function
$h_1(\cdot),\ h_2(\cdot)$	Hash function $h_1 : \{0,1\}^* \to \{0,1\}^l$, hash function $h_2 : \{0,1\}^* \to Z_p^*$.
x	Private key selected by S
$\oplus,\ \|\|$	Exclusive-or operation and concatenation operation

Authentication

(1) U inserts SC_i into a smart card reader, inputs ID_i, and PW_i, and imprints biometric B_i^* at the sensor. Then, SC_i computes $B_i = V_i \oplus PW_i \oplus ID_i$ and verifies whether the equation $d(B_i, B_i^{ast}) < \tau$ holds or not. If holds, SC_i computes $AID_i = h_1(B_i \oplus N_C) \oplus h_1(PW_i \oplus N_C) \oplus ID_i \oplus W_i$, selects a random number d_C and continues to compute $R_C = AID_i d_C P = h_2(x||ID_i) d_C P$, and $V_1 = h_1(ID_i||R_C||AID_i||T_C)$, and sends a message REQUEST $\{R_C, T_C, V_1, MID_i, R_i\}$ to S, where T_C is the current time.

(2) When receiving the message, S checks whether the transmission delay is within the allowed time interval ΔT. If $T_S - T_C < \Delta T$, S computes $N_S = x \oplus R_i$, derives ID_i by computing $MID_i \oplus h_1(N_S)$, and checks whether ID_i exists in database or not. If exists, S checks whether $h_1(ID_i||R_C||h_2(x||ID_i)||T_C) \overset{?}{=} V_1$. If holds, S selects a random number d_S and computes $Q_S = d_S P$ and $K_1 = h_2(x||ID_i)^{-1} d_S R_C = d_S d_C P$. Furthermore, S chooses a random number N_S^{New} and computes $R_i^* = h_1(K_1) \oplus x \oplus N_S^{New}$, $MID_i^* = h_1(K_1) \oplus ID_i \oplus h(N_S^{New})$, and $V_2 = h_1(MID_i^*||Q_S||K_1||R_i^*||ID_i)$. Finally, S sends the message CHALLENGE $\{Q_S, V_2, MID_i^*, R_i^*\}$ to U.

(3) After receiving the message, U computes $K_2 = d_C Q_S = d_C d_S P$ and checks whether $h_1(MID_i^*||Q_S||K_2||R_i^*||ID_i) \overset{?}{=} V_2$. If the equation is true, U computes $MID_i^{New} = MID_i^* \oplus h_1(K_2) ID_i \oplus h_1(N_S^{New})$, and $R_i^{New} = R_i^* \oplus h_1(K_2) x \oplus N_S^{New}$. Then, U updates the values of MID_i and R_i with the values of $MID_i^{New}$and R_i^{New}, respectively. Finally, U computes $V_3 = h_1(K_2||Q_S||ID_i)$, and the shared session key $SK = h_1(ID_i||Q_S||K_2)$, and sends a message RESPONSE $\{V_3\}$ to S.

(4) After receiving the message, S checks whether $h_1(K_1||Q_S||ID_i) \overset{?}{=} V_3$. If equal, S accepts the shared session key SK as $SK = h_1(ID_i||Q_S||K_1)$.

Password change

U inserts SC_i into the card reader, inputs identity ID_i, password PW_i and imprints his biometric B_i^* at the sensor. SC_i 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 holds, U keys a new password PW_i^{New} and imprints a new personal biometric B_i^{New}. Then, SC_i computes V_i^{new} and W_i^{New} as follows:

$V_i^{New} = PW_i^{New} \oplus B_i^{New} \oplus PW_i \oplus B_i \oplus V_i = PW_i^{New} \oplus B_i^{New} \oplus ID_i$

$W_i^{New} = h_1(B_i^{New} \oplus N_C) \oplus h_1(PW_i^{New} \oplus N_C) \oplus ID_i \oplus AID_i$ and updates SC_i's memory V_i, W_i by V_i^{New}, W_i^{New}.

Weaknesses of Arshad et al.'s scheme

This section shows that Arshad et al.'s scheme [27] has two security drawbacks, which are discussed in the following subsections. The following attacks are based on the assumptions that a malicious attacker $\mathcal{A}$ has completely monitor over the communication channel connecting U and S in login and authentication phase. So $\mathcal{A}$ can eavesdrop, modify, insert, or delete any message transmitted via public channel [31].

Not withstanding the off-line password guessing attack

The password and identity are low entropy [32, 33]. Therefore, $\mathcal{A}$ can guess a password PW_i' and an identity ID_i with the help of achieving values [34, 35] $\{V_i, W_i, R_i, MID_i, \tau, d(\cdot), E, n, P, Y, h_1(\cdot), h_2(\cdot)\}$ from the medical device and $\{R_C, T_C, V_1, MID_i, R_i\}$ from the login request message as follows:

(1) $\mathcal{A}$ guesses PW_i' and ID_i' and computes $AID_i' = h_1(V_i \oplus ID_i' \oplus PW_i' \oplus N_C) \oplus h_2(PW_i' \oplus N_C) \oplus ID_i' \oplus W_i$, $V_1' = h_1(ID_i'||R_C||AID_i'||T_C)$. Then, $\mathcal{A}$ checks $V_1' \overset{?}{=} V_1$.

(2) If the verification succeeds, considers ID_i' and PW_i' as the user's identity and password. Otherwise, he repeats (1).

If $\mathcal{A}$ successfully guesses the identity and the password of the patient, it will result into another attack. The detail of the attack is discussed as the next subsection.

Not withstanding the user impersonation attack

As described in the previous subsection, $\mathcal{A}$ can read [34, 35] the information $\{V_i, W_i, R_i, MID_i, \tau, d(\cdot), E, n, P, Y, h_1(\cdot), h_2(\cdot)\}$ stored in the smart card. After successfully guessing the password PW_i and ID_i, $\mathcal{A}$ can launch a user impersonation attack with the eavesdropped message $\{R_C, T_C, V_1, MID_i, R_i\}$ in the following:

(1) $\mathcal{A}$ generates a random number d_C' and computes $R_C' = AID_i d_C' P$, $V_1' = h_1(ID_i||R_C'||ADI_i||T_C')$. After that, he sends the REQUEST message $\{R_C', T_C', V_1', MID_i, R_i\}$ to S, where T_C' is the current timestamp.

(2) After checking the freshness of T_C', S derives N_S and ID_i and verifies $h_1(ID_i||R_C'||h_2(x||ID_i)||T_C') \overset{?}{=}$

V_1. Obviously, the equation will be held due to the true identity. S then continues to perform the original scheme without any detected. Finally, S delivers the CHALLENGE message $\{Q_S, V_2, MID_i^*, R_i^*\}$ to $\mathcal{A}$.

(3) $\mathcal{A}$ imitates what the patient were doing and computes V_3 and sends it to S, where $V_3 = h_1(d'_C Q_S||Q_S||ID_i)$. When receiving the value V_3, $\mathcal{A}$ will surely pass through S. As a result, S negotiates the session key $SK = h_1(ID_i||Q_S||d'_C Q_S)$ with $\mathcal{A}$ who masquerades as the legal patient.

Proposed scheme

This section presents a slight modification scheme to remedy the weaknesses of Arshad et al.'s scheme. The proposed scheme aims to propose an efficient improvement on Arshad et al.'s scheme to overcome the weaknesses of their scheme, while also retaining the original merits of their scheme. In the proposed scheme, in order to resist the off-line password guessing attack, we employ biometrics to conceal password. And we adopt Biohashing to protect biometrics of patients, which can resolve high false rejection and hence decrease denial of service access probability [36, 37]. And biohashing is very efficient and lightweight as compared to modular exponentiation and elliptic curve point multiplication [38, 39]. The proposed scheme also contains three phases: registration, login and authentication and password updating (Fig. 1).

Registration

(1) The patient U inputs his biometric B_i, identity ID_i and password PW_i. Then, U calculates $MP_i = PW_i \oplus H(B_i)$ and submits $\{ID_i, MP_i\}$ to the server S.

(2) When receiving the message, S computes $AID_i = ID_i \oplus h_2(x)$, $V_i = h_1(ID_i||MP_i)$ and issues a smart card SC_i which contains the information $\{AID_i, V_i, h_1(\cdot), h_2(\cdot), H(\cdot)\}$ to U.

Login and Authentication

(1) U inserts SC_i into a card reader and keys his identity ID_i, password PW_i and biometric B_i. SC_i computes $h_1(ID_i||PW_i \oplus H(B_i))$ and verifies whether it is equal to the value V_1. If true, U passes through the verification. Then, SC_i selects a random number d_u and computes $K = h_1(ID_i||ID_i \oplus AID_i)$, $M_1 = K \oplus d_u P$, $M_2 = h_1(ID_i||T_1||d_u P)$, and transmits $\{M_1, M_2, AID_i, T_1\}$ to S.

(2) When receiving the login request, S first examines whether $|T_1 - T_c| < \Delta T$, where T_c is the current timestamp of the S. If holds, S uses his private key x to derive ID_i by computing $M_1 \oplus h_2(x)$, he then computes $d_u P = K \oplus M_1$ and checks $h(ID_i||T_1||d_u P) \overset{?}{=} M_2$. If correct, S then generates a random number d_s and computes $M_3 = K \oplus d_s P$, $SK = d_s d_u P$, $M_4 = h_1(K||T_2||SK||d_u P)$, where T_2 is the current timestamp. At last, S sends the message $\{M_3, M_4, T_2\}$ to U.

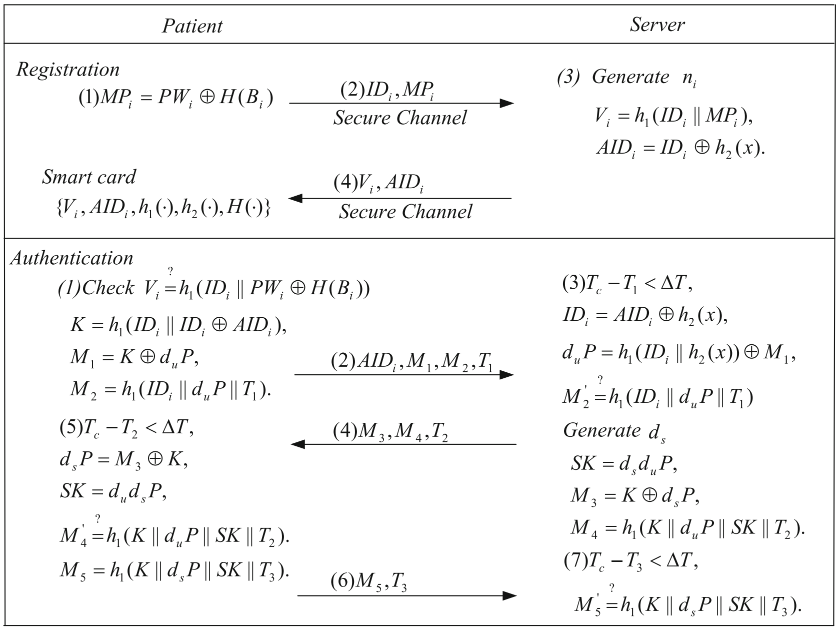
Patient
Server
Registration
$(1) MP_i = PW_i \oplus H(B_i)$
$(2) ID_i, MP_i$
Secure Channel
(3) Generate n_i
$V_i = h_1(ID_i \| MP_i)$,
$AID_i = ID_i \oplus h_2(x)$.
Smart card
$\{V_i, AID_i, h_1(\cdot), h_2(\cdot), H(\cdot)\}$
$(4) V_i, AID_i$
Secure Channel
Authentication
(1)Check $V_i \overset{?}{=} h_1(ID_i \| PW_i \oplus H(B_i))$
$K = h_1(ID_i \| ID_i \oplus AID_i)$,
$M_1 = K \oplus d_u P$,
$M_2 = h_1(ID_i \| d_u P \| T_1)$.
$(2) AID_i, M_1, M_2, T_1$
$(3) T_c - T_1 < \Delta T$,
$ID_i = AID_i \oplus h_2(x)$,
$d_u P = h_1(ID_i \| h_2(x)) \oplus M_1$,
$M'_2 \overset{?}{=} h_1(ID_i \| d_u P \| T_1)$
Generate d_s
$SK = d_s d_u P$,
$M_3 = K \oplus d_s P$,
$M_4 = h_1(K \| d_u P \| SK \| T_2)$.
$(4) M_3, M_4, T_2$
$(5) T_c - T_2 < \Delta T$,
$d_s P = M_3 \oplus K$,
$SK = d_u d_s P$,
$M'_4 \overset{?}{=} h_1(K \| d_u P \| SK \| T_2)$.
$M_5 = h_1(K \| d_s P \| SK \| T_3)$.
$(6) M_5, T_3$
$(7) T_c - T_3 < \Delta T$,
$M'_5 \overset{?}{=} h_1(K \| d_s P \| SK \| T_3)$.

Fig. 1 Registration and authentication phase of the enhanced scheme

Table 2 BAN logic notations

$A\vert\equiv X$	A believes a statement X
$U \overset{K}{\leftrightarrow} S$	Share a key K between user and sever
$\#X$	X is fresh
$A \lhd X$	A sees X
$A\vert\sim X$	A said X
$\{X,\ Y\}_K$	X and Y are encrypted with the key K.
$(X,\ Y)_K$	X and Y are hashed with the key K.
$< X >_K$	X is xored with the key K

(3) Upon receiving the message, U first checks the freshness of T_2. Then, U retrieves d_sP by computing $M_3 \oplus K$ and computes $SK = d_u d_s P$, $M_4' = h_1(K||d_uP||SK||T_2)$ to verify whether M_4' is equal to the received M_4. If holds, U computes $M_5 = h_1(K||d_sP||SK||T_3)$ and then sends the message $\{M_5,\ T_3\}$ to S, where T_3 is the current timestamp.

(4) After receiving $\{M_5,\ T_3\}$, S verifies whether $|T_3 - T_c| < \Delta T$ and $M_5' = h_1(K||d_sP||SK||T_3) \overset{?}{=} M_5$. If both conditions hold, S authenticates U and accepts SK as the session key for further operations.

Password change

If U doubts his password may be leaked, he can alter the old password to a new one as follows. U inserts his SC_i into the device and submits his ID_i, PW_i and B_i. Then SC_i verifies whether $h_1(ID_i||PW \oplus H(B_i)) \overset{?}{=} V_i$. If valid, U inputs a new password PW^{new}, SC_i calculates $V_i^{new} = h_1(ID_i||PW^{new} \oplus H(B_i))$ then replaces V_i with V_i^{new}.

Analysis security

This section conducts a cryptanalysis of the enhanced scheme both through Burrows-Abadi-Needham (BAN) logic [30] and security features.

Proofing scheme with BAN logic

BAN logic [30] is a set of rules for defining and analyzing information exchange schemes (Table 2). It helps its users determine whether exchanged information is trustworthy, secured against eavesdropping, or both. It has been highly successful in analyzing the security of authentication schemes. We first introduce some notations and logical postulates of BAN logic used in our scheme.

(1) BAN logical postulates

a. Message-meaning rule: $\frac{A|\equiv A\overset{K}{\leftrightarrow}B,\, A\lhd\{X\}_K}{A|\equiv B\sim X}$: if A believes that K is shared by A and B, and sees X encrypted with K, then A believes that B once said X.

b. Nonce-verification rule: $\frac{A|\equiv\#X,\, A|\equiv B|\sim X}{A|\equiv B|\equiv X}$: if A believes that X could have been uttered only recently and that B once said X, then A believes that B believes X.

c. The belief rule: $\frac{A|\equiv X,\ A|\equiv Y}{A|\equiv(X,\ Y)}$: if A believes X and Y, then A believes $(X,\ Y)$.

d. Fresh conjuncatenation rule: $\frac{A|\equiv\#X}{A|\equiv\#(X,\ Y)}$: if A believes freshness of X, B believes freshness of $(X,\ Y)$.

e. Jurisdiction rule: $\frac{A|\equiv B\Rightarrow X,\ A|\equiv B|\equiv X}{A|\equiv X}$: if A believes that B has jurisdiction over X and A trusts B on the truth of X, then A believes X.

(2) Idealized scheme

$$U: \ < d_uP >_{U\overset{K}{\longleftrightarrow}S}, < ID_i >_{h_2(x)}, (ID_i, d_uP, T_1), (U \overset{SK}{\longleftrightarrow} S, d_sP, T_3)_{U\overset{K}{\longleftrightarrow}S}$$

$$S: \ < d_sP >_{U\overset{K}{\longleftrightarrow}S}, (U \overset{SK}{\longleftrightarrow} S, d_uP, T_2)_{U\overset{K}{\longleftrightarrow}S}$$

(3) Establishment of security goals

g_1. $S|\equiv U|\equiv U \overset{SK}{\longleftrightarrow} S$

g_2. $S|\equiv U \overset{SK}{\longleftrightarrow} S$

g_3. $U|\equiv S|\equiv U \overset{SK}{\longleftrightarrow} S$

g_4. $U|\equiv U \overset{SK}{\longleftrightarrow} S$

(4) Initiative premises

p_1. $U|\equiv \#d_u$

p_2. $S|\equiv \#d_s$

p_3. $U|\equiv U \overset{K}{\longleftrightarrow} S$

p_4. $S|\equiv U \overset{K}{\longleftrightarrow} S$

p_5. $U|\equiv S \Rightarrow (U \overset{SK}{\longleftrightarrow} S)$

p_6. $S|\equiv U \Rightarrow (U \overset{SK}{\longleftrightarrow} S)$

(5) Scheme analysis

a_1. Since p_3 and $U \lhd (U \overset{SK}{\longleftrightarrow} S,\ d_uP,\ T_2)_{U\overset{K}{\longleftrightarrow}S}$, by the message-meaning rule, we get: $U| \equiv S| \sim (U \overset{SK}{\longleftrightarrow} S,\ d_uP,\ T_2)$.

a_2. Since p_1 and a_1, by the fresh conjuncatenation and nonce-verification rules, we get: $U| \equiv S| \equiv (U \overset{SK}{\longleftrightarrow} S,\ d_uP,\ T_2)$.

g_1. Since a_2, by the belief rule, we get: $U| \equiv S| \equiv U \overset{SK}{\longleftrightarrow} S$.

g_2. Since p_5 and g_1, by the jurisdiction rule, we get: $U| \equiv U \overset{SK}{\longleftrightarrow} S$.

a_3. Since p_4 and $S \lhd (U \overset{SK}{\longleftrightarrow} S,\ d_sP,\ T_3)_{U\overset{K}{\longleftrightarrow}S}$, by the message-meaning rule, we get: $S| \equiv U| \sim (U \overset{SK}{\longleftrightarrow} S,\ d_sP,\ T_3)$.

Table 3 Functionality comparison

	Ours	Arshad et al. [27]	Tan et al. [26]	Awasthi et al. [24]	Wen et al. [13]
User anonymity	Yes	Yes	Yes	No	Yes
Mutual authentication	Yes	Yes	Yes	Yes	Yes
The session key perfect forward secrecy	Yes	Yes	-	-	Yes
Insider attack	Yes	Yes	Yes	Yes	Yes
Impersonation attack	Yes	No	Yes	-	-
Off-line password guessing attack	Yes	No	Yes	Yes	Yes
Replay attack	Yes	Yes	No	Yes	Yes
Modification attack	Yes	Yes	Yes	-	-

a_4. Since p_2 and a_3, by the fresh conjuncatenation and nonce-verification rules, we get: $S| \equiv U| \equiv (U \overset{SK}{\longleftrightarrow} S,\ d_sP,\ T_3)$.

g_3. Since a_4, by the belief rule, we get: $S| \equiv U| \equiv (U \overset{SK}{\longleftrightarrow} S,\ d_sP,\ T_3)$.

g_4. Since g_3 and p_6, by the jurisdiction rule, we get: $S| \equiv U \overset{SK}{\longleftrightarrow} S$.

Security analysis

This section shows the enhanced scheme has the ability to endure different security attacks including the aforementioned attacks found in Arshad et al.'s scheme. The following attacks are based on the assumptions that a malicious attacker $\mathcal{A}$ has completely control the whole communication channel connecting the patients and the telecare server in login and authentication phase. So $\mathcal{A}$ can eavesdrop, modify, insert, or delete any message transmitted via public channel [31].

User anonymity

The patient's identity ID_i is concealed all the transmitted messages and is protected by one-way hash functions. If $\mathcal{A}$ attempts to derive ID_i, he needs to know the server's private key x or the random numbers generated by U and S. Obviously, this values are secret only known by U and S. Therefore, it is impossible to track the patient who is involved in the authentication session.

Insider attack

The patient registers to S by presenting $PW_i \oplus H(B_i)$ instead of plaintext PW_i. Since B_i is unknown to the insider, it will be difficult to retrieve PW_i from $PW_i \oplus H(B_i)$. Therefore, a privileged insider S cannot attain the plain-text password and hence he cannot pretend the patient to login other telecare servers.

Off-line password guessing attack

Assume that $\mathcal{A}$ reads [34, 35] the information $\{V_i,\ AID_i\}$ stored in the smart card and tries to guess a password in an off-line manner. To verify the correctness of password, $\mathcal{A}$ needs to know patients's ID_i and biometric B_i at the same time. To obtain ID_i from AID_i, the telecare server's private key x is needed. Since $\mathcal{A}$ cannot know the biometric B_i and x which is only with U and S, respectively, it is hard for $\mathcal{A}$ to plot an off-line password guessing attack with smart card.

Impersonation attack

$\mathcal{A}$ does not impersonate a legal patient to server since he cannot generate a valid login request $\{M_1,\ M_2,\ AID_i,\ T_1\}$ without the knowledge of U's identity ID_i and S's private key x. Both the two values ID_i and x are unknown to $\mathcal{A}$. Similarly, $\mathcal{A}$ cannot impersonate as a server to cheat a legal patient without knowledge of x. Only when $\mathcal{A}$ knows x he will derive ID_i from intercepted messages. But x is the secret key of S, $\mathcal{A}$ cannot know. In a word, it is infeasible for $\mathcal{A}$ to launch an impersonation attack.

Table 4 Performance comparison

	Ours	Arshad et al. [27]	Tan et al. [26]	Awasthi et al. [24]	Wen et al. [13]
Registration	$3T_h$	$4T_h$	$3T_h$	$3T_h$	$3T_h$
Login and authentication	$4T_{pm} + 11T_h$	$4T_{pm} + 15T_h + 2T_m +$ $+1T_{inv}$	$6T_{pm} + 11T_h$	$6T_{pm} + 9T_h$	$1T_m + 4T_s + 8T_e +$ $+1T_F + 5T_h$
Password change	$3T_h$	$4T_h$	$4T_h$	$4T_h$	$4T_h$

The session key perfect forward secrecy

Even if the patient's password PW_i and server's private key x are compromised by $\mathcal{A}$, the session key SK for the previous sessions is still kept unrevealed. On the one hand, the password PW_i and server's private key x are not utilized for computing the session key. On the other hand, it is impractical to compute $SK = d_u d_s P$ without knowledge of d_u and d_s. As a result, the enhanced scheme achieves the session key perfect forward secrecy.

Mutual authentication

U validates S's message $\{AID_i,\ M_1,\ M_2,\ T_1\}$ by checking whether the timestamp T_1 and the condition $M_2' = M_2$ are valid. S validates U's message $\{M_3,\ M_4,\ T_2\}$ by checking whether the timestamp T_2 and the condition $M_2' = M_2$ hold.

Replay attack

Assume that $\mathcal{A}$ intends to resend the old message $\{M_1,\ M_2,\ AID_i,\ T_1\}$ to login to S. The attack will be immediately detected by S by verifying the freshness of T_1. Besides, S will also discover the forged message by verifying the correctness of the value $M_2 = h_1(ID_i||d_u P||T_1)$. Therefore, it is impossible for $\mathcal{A}$ to plot the replay attack.

Modification attack

Both the patient's identity ID_i and the server's private key x are hidden in all the transmitted messages. Any forged messages will be examined by U or S. It seems impossible for $\mathcal{A}$ to intercept the transmitted messages and hence modify them without knowledge of the two values.

Functionality and performance comparisons

In this section, we compare the functionality and performance analyses of the enhanced scheme with the previous related schemes [13, 24, 26, 27]. Table 3 shows that the enhanced scheme is more secure than other related schemes. In the performance comparison, define pm, m, inv, s, F, e and h be the time for performing an elliptic curve point multiplication, a modular multiplication, a modular inversion, a symmetric encryption/decryption, a pseudo-random function, a modular exponentiation and a one-way hash function. From Table 4 we can see that the overall computational cost for the enhanced scheme is less computationally costly than those of schemes [13, 24, 26, 27].

Conclusion

We have discussed the security of Arshad et al.'s scheme and discovered that their scheme was vulnerable to off-line password guessing attack which leads to an adversary could impersonate as a legal user to access any services provided by telecare server. We employ hash function, ECC nonce and biometric based authenticated key exchange scheme as the primitives to improve the security and efficiency of Arshad et al.'s scheme. The enhanced scheme not only satisfies many security features but also has the lowest computational cost among other related schemes.

Acknowledgments The authors would like to thank all the anonymous reviewers for their helpful advice. This paper is supported by the National Natural Science Foundation of China (Grant No. 61121061), the Beijing Natural Science Foundation (Grant No. 4142016), and the Asia Foresight Program under NSFC Grant (Grant No. 61411146001).

References

1. Leng, L., Teoh, A.B.J., Li, M., Khan, M.K.: A remote cancelable palmprint authentication protocol based on multi-directional two-dimensional palmphasor-fusion. *Sec. Commun. Netw.* doi:10.1002/sec.900, 2013.
2. He, D.B., Kumar, N., Chilamkurti, N., Lee, J.H., Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol. *J. Med. Syst.* 38(10):1–6, 2014.
3. He, D.B., and Zeadally, S., Authentication protocol for ambient assisted living system. *IEEE Commun. Mag.* 53(1):2–8, 2015.
4. Lu, Y.R., Li, L.X., Peng, H.P., Yang, X., Yang, Y.X.: A lightweight ID based authentication and key agreement protocol for multi-server architecture, *Int. J. Distrib. Sens. N.*, Article ID 635890, 1-16, 2015. in press, 2015.
5. Lu, Y.R., Li, L.X., Yang, Y.X.: Robust and efficient authentication scheme for session initiation protocol.*Math. Probl. Eng*2015, Article ID 894549, 1-16, in press, 2015.
6. 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.
7. He, D., Chen, J., Zhang, R., A more secure authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(3):1989–1995, 2012.
8. Wei, J., Hu, X., Liu, W., An improved authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(6):3597–3604, 2012.
9. Zhu, Z., An efficient authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(6):3833–3838, 2012.
10. Rivest, R., Shamir, A., Adleman, L., A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* 21(2):120–126, 1978.
11. Wu, F., and Xu, L.L., Security analysis and improvement of a privacy authentication scheme for telecare medical information systems. *J. Med. Syst.* 37:1–9, 2013.

12. Jiang, Q., Ma, J.F., Ma, Z., Li, G.S., A privacy enhanced authentication scheme for telecare medical information systems. *J. Med. Syst.* 37(1):1–8, 2013.
13. Wen, F.T., and Guo, D.l., An improved anonymous authentication scheme for telecare medical information systems. *J. Med. Syst.* 38(5):1–11, 2014.
14. Kim, K.W., and Lee, J.D., On the security of two remote user authentication schemes for telecare medical information systems. *J. Med. Syst.* 38(5):1–11, 2014.
15. Giri, D., Maitra, T., Amin, R., An efficient and robust RSA-based remote user authentication for telecare medical information systems. *J. Med. Syst.* 39(1):1–9, 2015.
16. Islam, S.K.H., and Khan, M.K., Cryptanalysis and improvement of authentication and key agreement protocols for telecare medicine information systems. *J. Med. Syst.* 38(10):1–16, 2014.
17. Li, C.T., and Hwang, M.S., An efficient biometrics-based remote user authentication scheme using smart cards. *J. Netw. Comput. Appl.* 33(1):1–5, 2010.
18. Das, A.K., and Goswami, A., An enhanced biometric authentication scheme for telecare medicine information systems with nonce using chaotic hash function. *J. Med. Syst.* 38(6):27, 2014.
19. Maitra, T., and Giri, D., An efficient biometric and password-based remote user authentication using smart card for telecare medical information systems in multi-server environment. *J. Med. Syst.* 38(12):1–19, 2014.
20. 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(5):1–6, 2013.
21. 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(6):1–12, 2014.
22. Li, X.L., Wen, Q.Y., Li, W.M., Zhang, H., Jin, Z.P., Secure privacy-preserving biometric authentication scheme for telecare medicine information systems. *J. Med. Syst.* 38(11):1–8, 2014.
23. He, D.B., and Wang, D.: Robust biometrics-based authentication scheme for multi-server environment, *IEEE. Syst. J.* doi:10.1109/JSYST.2014.2301517, 2014.
24. Awasthi, A.K., and Srivastava, K., A biometric authentication scheme for telecare medicine information systems with nonce. *J. Med. Syst.* 37(5):1–4, 2013.
25. 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.* 38(5):1–11, 2014.
26. Tan, Z., A user anonymity preserving three-factor authentication scheme for telecare medicine information systems. *J. Med. Syst.* 38(3):1–9, 2014.
27. Arshad, H., and Nikooghadam, M., Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems. *J. Med. Syst.* 38(12):1–12, 2014.
28. Miller, V. *Uses of elliptic curves in cryptography. Advances in CryptologyCRYPTO'85 Proceedings.* pp. 417–426. Berlin Heidelberg: Springer Verlag LNCS 218, 1986.
29. Koblitz, N., Elliptic curve cryptosystems. *Math. Comp.* 48:203–209, 1987.
30. Burrow, M., Abadi, M., Needham, R., A logic of authentication. *ACM Trans. Comput. Syst.* 8:18–36, 1990.
31. Lamport, L., Password authentication with insecure communication. *Commun. ACM* 24(11):770–772, 1981.
32. He, D.B., Zhang, Y.Y., Chen, J.H., Cryptanalysis and improvement of an anonymous authentication protocol for wireless access networks. *Wirel. Pers. Commun.* 74(2):229–243, 2014.
33. He, D.B., and Wu, S.H., Security flaws in a smart card based authentication scheme for multi-server environment. *Wirel. Pers. Commun.* 70(1):323–329, 2013.
34. Messerges, T.S., Dabbish, E.A., Sloan, R.H., Examining smart-card security under the threat of power analysis attacks. *IEEE Trans. Comput.* 51(5):541–552, 2002.
35. Kocher, P., Jaffe, J., Jun, B., Differential power analysis. *Adv. Cryptology CRYPTO'99 LNCS* 1666:388–397, 1999b.
36. Belguechi, R., Rosenberger, C., Ait-Aoudia, S., Biohashing for securing minutiae template. *Int. Conf. Pattern Recognition* (ICPR2010), 1168–1171, 2010.
37. Lumini, A., and Nanni, L., An improved biohashing for human authentication. *Pattern Recogn.* 40(3):1057–1065, 2007.
38. Inuma, M., Otsuka, A., Imai, H., Theoretical framework for constructing matching algorithms in biometric authentication systems. *Adv. Biometrics* 5558:806–815, 2009.
39. Das, A.K., and Goswami, A., An enhanced biometric authentication scheme for telecare medicine information systems with nonce using chaotic hash function. *J. Med. Syst.* 38(6): 27, 2014.