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
© The Author(s) 2015. This article is published with open access at Springerlink.com

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
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 $AILD_i = h_2(x||ID_i)$, $V_i = MPW_i \oplus MB_i \oplus ID_i = PW_i \oplus B_i \oplus ID_i$, and $W_i = h_1(MB_i) \oplus h_1(MPW_i) \oplus ID_i \oplus AILD_i$. 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 $h_1 : \{0, 1\}^* \rightarrow \{0, 1\}^l$, hash function $h_2 : \{0, 1\}^* \rightarrow \mathbb{Z}_p^n$. |
| $x$ | Private key selected by $S$ |
| $\oplus, ||$ | Exclusive-or operation and concatenation operation |
(1) U inserts $SC_i$ into a smart card reader, inputs $ID_1$, 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 $d(B_i, B_i^{ass}) < \tau$ 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 $R_C = AID_i \cdot d_C \cdot P = h_2(x || ID_i) \cdot d_C \cdot P$, and $V_i = h_1(ID_i || R_C || AID_i || T_C)$, and sends a message REQUEST $\{R_C, T_C, V_i, MID_i, R_i\}$ 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 $\Delta T$. If $T_S - T_C < \Delta T$, $S$ computes $N_S = x \oplus R_i$, derives $ID_1$ by computing $MID_i \oplus h_1(N_S)$, and checks whether $ID_1$ exists in database or not. If exists, $S$ checks whether $h_1(ID_1 || R_C || h_2(x || ID_i)) || T_C) \equiv V_i$. If holds, $S$ selects a random number $d_S$ and computes $Q_S = d_S \cdot P$ and $K_1 = h_2(x || ID_i)^{-1} \cdot d_S \cdot RC = d_S \cdot P$. Furthermore, $S$ chooses a random number $N^{\text{New}}_S$ and computes $R^*_S = h_1(K_1) \oplus x \oplus N^{\text{New}}_S$, $MID^*_i = h_1(K_1) \oplus ID_i \oplus h(N^{\text{New}}_S)$, and $V_2 = h_1(MID^*_i || Q_S || K_1 || R^*_S || ID_i)$. Finally, $S$ sends the message CHALLENGE $\{Q_S, V_2, MID^*_i, R^*_S\}$ to $U$.

(3) After receiving the message, $U$ computes $K_2 = d_C \cdot Q_S = d_C \cdot d_S \cdot P$ and checks whether $h_1(MID^*_i || Q_S || K_2 || R^*_S || ID_i) \equiv V_2$. If the equation is true, $U$ computes $MID^{\text{New}}_i = MID^*_i \oplus h_1(K_2) \cdot ID_i \oplus h_1(N^{\text{New}}_S)$, and $R^{\text{New}}_S = R^*_S \oplus h_1(K_2) \oplus x \oplus N^{\text{New}}_S$. Then, $U$ updates the values of $MID_i$ and $R_i$ with the values of $MID^{\text{New}}_i$ and $R^{\text{New}}_S$, 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 $h_1(K_1 || Q_S || ID_i) \equiv V_3$. If equal, $S$ accepts the shared session key $SK = h_1(ID_i || Q_S || K_1)$.

Password change

$U$ inserts $SC_i$ into the card reader, inputs identity $ID_1$, 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 $d(B_i, B_i^{ass}) < \tau$ holds or not. If holds, $U$ keys a new password $PW^{\text{New}}_i$ and imprints a new personal biometric $B^{\text{New}}_i$. Then, $SC_i$ computes $V^{\text{new}}_i$ and $W^{\text{New}}_i$ as follows:

$$V^{\text{new}}_i = PW^{\text{New}}_i \oplus B^{\text{New}}_i \oplus PW_i \oplus B_i \oplus V_i = PW^{\text{New}}_i \oplus B^{\text{New}}_i \oplus ID_i$$

$$W^{\text{New}}_i = h_1(B^{\text{New}}_i \oplus N_C) \oplus h_1(PW^{\text{New}}_i \oplus N_C) \oplus ID_i \oplus AID_i$$

and updates $SC_i$’s memory $V_i$, $W_i$ by $V^{\text{New}}_i$, $W^{\text{New}}_i$.

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 $A$ has completely monitor the communication channel connecting $U$ and $S$ in login and authentication phase. So, $A$ can eavesdrop, modify, insert, or delete any message transmitted via public channel [31].

Notwithstanding the off-line password guessing attack

The password and identity are low entropy [32, 33]. Therefore, $A$ can guess a password $PW'_i$ and an identity $ID'_i$ with the help of achieving values [34, 35] $\{V_i, W_i, R_i, MID_i, T_C, V_i, MID_i, R_i\}$ from the medical device and $\{R_C, T_C, V_i, MID_i, R_i\}$ from the login request message as follows:

(1) $A$ guesses $PW'_i$ and $ID'_i$ and computes $AID'_i = h_1(V_i || ID'_i || PW'_i || N_C) \oplus h_2(PW'_i || N_C) \oplus ID'_i || W_i$, $V'_i = h_1(ID'_i || R_C || AID'_i || T_C)$. Then, $A$ checks $V'_i \equiv V_i$.

(2) If the verification succeeds, considers $ID'_i$ and $PW'_i$ as the user’s identity and password. Otherwise, he repeats (1).

If $A$ 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, $A$ can read [34, 35] the information $\{V_i, W_i, R_i, MID_i, T_C, V_i, MID_i, R_i\}$ stored in the smart card. After successfully guessing the password $PW_i$ and $ID_i$, $A$ can launch a user impersonation attack with the xedropped message $\{R_C, T_C, V_i, MID_i, R_i\}$ in the following:

(1) $A$ generates a random number $d'_C$ and computes $R'_C = AID_i \cdot d'_C \cdot P$, $V'_i = h_1(ID_i || R'_C || AID_i || T'_C)$. After that, he sends the REQUEST message $\{R'_C, T'_C, V'_i, MID_i, R_i\}$ 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 $h_1(ID_i || R'_C || h_2(x || ID_i)) || T'_C) \equiv$
V1. 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 \{QS, VID, R_i\} to A.

(3) A imitates what the patient were doing and computes V3 and sends it to S, where V3 = h1(dC||QS||ID) with 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 Bi, identity IDi and password PWi. Then, U calculates MPi = PWi ⊕ H(Bi) and submits \{IDi, MPi\} to the server S.

(2) When receiving the message, S computes AIDi = IDi ⊕ h2(x), V1 = h1(IDi||MPi) and issues a smart card SCi which contains the information \{AIDi, V1, h1(), h2(), H()\} to U.

Login and Authentication

(1) U inserts SCi into a card reader and keys his identity IDi, password PWi and biometric Bi. SCi computes h1(IDi||PWi ⊕ H(Bi)) and verifies whether it is equal to the value V1. If true, U passes through the verification. Then, SCi selects a random number du and computes K = h1(IDi||IDi ⊕ AIDi), M1 = K ⊕ duP, M2 = h1(IDi||T1||duP), and transmits \{M1, M2, AIDi, T1\} to S.

(2) When receiving the login request, S first examines whether \(|T1 - Tc| < \Delta T\), where Tc is the current timestamp of the S. If holds, S uses his private key x to derive IDi by computing M1 ⊕ h2(x), he then computes duP = K ⊕ M1 and checks h(IDi||T1||duP) ≠ M2. If correct, S then generates a random number ds and computes M3 = K ⊕ dsP, SK = dsduP, M4 = h1(K||T2||SK||duP), where T2 is the current timestamp. At last, S sends the message \{M3, M4, T2\} to U.
If U Password change U old password to a new one as follows. h {

(4) Upon receiving the message, U first checks the freshness of T2. Then, U retrieves d4 P by computing M4 = K = d4d4 P, M′4 = h1 (K || d4 P || SK || T2) to verify whether M′4 is equal to the received M4. If holds, U computes M5 = h1 (K || d4 P || SK || T3) and then sends the message {M5, T3} to S, where T3 is the current timestamp.

(3) After receiving {M5, T3}, S verifies whether |T3 - T2| < δT and M′5 = h1 (K || d4 P || SK || T3) = M5. 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 SCj into the device and submits his IDi, PWi and B1. Then SCj verifies whether h1 (IDi || PWi ⊕ H(B1)) = Vi. If valid, U inputs a new password PWnew, SCj calculates V′i new = h1 (IDi || PWnew ⊕ H(B1)) then replaces V with V′i new.

Analysis security

This section conducts a cryptanalytical study 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: A ||= B ||= X, A ||= X; if A believes that X is shared by A and B, and sees X encrypted with K, then A believes that B once said X.

b. Nonce-verification rule: A ||= X, A ||= 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: A ||= Y; if A believes X and Y, then A believes (X, Y).

d. Fresh conjunctuation rule: A ||= X; if A believes freshness of X, B believes freshness of (X, Y).

e. Jurisdiction rule: A ||= B ||= X, A ||= 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: < d4 P > U K S, IDi > h2 (x) S, d4 P, T3 U K S
S: < d4 P > U K S, d4 P, T2 U K S

(3) Establishment of security goals

g1. S ||= U ||= U K S

g2. S ||= U K S

g3. U ||= S ||= U K S

g4. U ||= U K S

(4) Initiative premises

p1. U ||= d4
p2. S ||= d4
p3. U ||= U K S
p4. S ||= U K S
p5. U ||= S ||= U K S
p6. S ||= U ||= U K S

(5) Scheme analysis

a1. Since p1 and U << (U K S, d4 P, T2) U K S, by the message-meaning rule, we get: U ||= S ||= U K S.

a2. Since p1 and a1, by the fresh conjunctuation and nonce-verification rules, we get: U ||= S ||= (U K S, d4 P, T2).

g1. Since a2, by the belief rule, we get: U ||= S ||= U K S.

a2. Since p5 and g1, by the jurisdiction rule, we get: U ||= U K S.

a3. Since p4 and S << (U K S, d4 P, T3) U K S, by the message-meaning rule, we get: S ||= U ||= (U K S, d4 P, T3).
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                | No              | Yes                 | Yes             |
| Mutual authentication  | Yes  | Yes                | Yes             | Yes                 | Yes             |
| The session key perfect forward secrecy | Yes  | Yes                | -               | -                   | Yes             |
| Insider attack         | Yes  | No                 | Yes             | Yes                 | Yes             |
| Impersonation attack   | Yes  | No                 | Yes             | Yes                 | Yes             |
| Off-line password guessing attack | Yes  | No                 | Yes             | Yes                 | Yes             |
| Replay attack          | Yes  | Yes                | No              | Yes                 | Yes             |
| Modification attack    | Yes  | Yes                | Yes             | -                   | -               |

\[a_4. \text{ Since } p_2 \text{ and } a_3, \text{ by the fresh conjunctenation and nonce-verification rules, we get: } S| ≡ U| ≡ (U ←← S, d_P, T_3).\]

\[g_3. \text{ Since } a_4, \text{ by the belief rule, we get: } S| ≡ U| ≡ (U ←← S, d_P, T_3).\]

\[g_4. \text{ Since } g_3 \text{ and } p_6, \text{ by the jurisdiction rule, we get: } S| ≡ U \stackrel{SK}{←←} S.\]

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 \(A\) has completely control the whole communication channel connecting the patients and the telecare server in login and authentication phase. So \(A\) 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 \(A\) 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.

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 | \(4T_{pm} + 11T_h\) | \(4T_{pm} + 15T_h + 2T_m + 1T_{inv}\) | \(6T_{pm} + 11T_h\) | \(6T_{pm} + 9T_h\) | \(11T_m + 4T_x + 8T_e + 1T_{inv}\) |
| 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 $A$, 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 $SK = d_u d_t P$ without knowledge of $d_u$ and $d_t$. 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 $A$ 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 $A$ 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 $A$ 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).

Open Access This article is distributed under the terms of the Creative Commons Attribution License which permits any use, distribution, and reproduction in any medium, provided the original author(s) and the source are credited.

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, 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.I., 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 scheme 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 a biometric-based authentication scheme for telecare medical information systems. J. Med. Syst. 38(10):1–12, 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 medical 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 cards 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 medical 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 medical 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 medical 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/JYST.2014.2301517, 2014.

24. Awasthi, A.K., and Srivastava, K., A biometric authentication scheme for telecare medical 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 medical 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 medical 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 medical information systems with nonce using chaotic hash function. J. Med. Syst. 38(6):27, 2014.