J Med Syst (2014) 38:41
DOI 10.1007/s10916-014-0041-1

Security Enhancement of a Biometric based Authentication Scheme for Telecare Medicine Information Systems with Nonce

Dheerendra Mishra · Sourav Mukhopadhyay · Saru Kumari · Muhammad Khurram Khan · Ankita Chaturvedi

Received: 25 October 2013 / Accepted: 18 March 2014 / Published online: 26 April 2014

Abstract Telecare medicine information systems (TMIS) present the platform to deliver clinical service door to door. The technological advances in mobile computing are enhancing the quality of healthcare and a user can access these services using its mobile device. However, user and Telecare system communicate via public channels in these online services which increase the security risk. Therefore, it is required to ensure that only authorized user is accessing the system and user is interacting with the correct system. The mutual authentication provides the way to achieve this. Although existing schemes are either vulnerable to attacks or they have higher computational cost while an scalable authentication scheme for mobile devices should be secure and efficient. Recently, Awasthi and Srivastava presented a biometric based authentication scheme for TMIS with nonce. Their scheme only requires the computation of the hash and XOR functions.pagebreak Thus, this scheme fits for TMIS. However, we observe that Awasthi and Srivastava's scheme does not achieve efficient password change phase. Moreover, their scheme does not resist off-line password guessing attack. Further, we propose an improvement of Awasthi and Srivastava's scheme with the aim to remove the drawbacks of their scheme.

Keywords E-medicine · Telecare Medicine Information Systems · Smart card · Password · Biometric

Introduction

Telecare medicine information system (TMIS) provides certain healthcare services, which become a feasible solution to the continuously rising demand in medical and healthcare sector. These health care services allow delivering personal health assistance to the patients' homes [1]. Most of the medical institutes are developing medical information systems to facilitate connected health care services. This connected health care provides an opportunity to improve financial and clinical performance. The technological advances in mobile computing are enhancing the quality of healthcare in the management of chronic disease. As a result, the patients can access healthcare related information on their mobile device. However, the user accesses the Telecare system via Internet (public network), which is subject to security risks. Therefore, user and server should establish authorized and secure connection in the beginning of these services.

The smart card based authentication scheme provides secure and authorized connection between the remote user and server [2, 3]. In recent time, many authentication protocols have been proposed for TMIS [4–21]. In general,

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

D. Mishra (✉) · S. Mukhopadhyay · A. Chaturvedi
Department of Mathematics, Indian Institute of Technology Kharagpur, Kharagpur 721 302, India
e-mail: dheerendra@maths.iitkgp.ernet.in

S. Mukhopadhyay
e-mail: sourav@maths.iitkgp.ernet.in

A. Chaturvedi
e-mail: ankita@maths.iitkgp.ernet.in

S. Kumari
Department of Mathematics, Agra College, Agra, Dr. B. R. A. University, Agra, Uttar Pradesh, India
e-mail: saryusiirohi@gmail.com

M. K. Khan
Center of Excellence in Information Assurance,
King Saud University, Riyadh, Kingdom of Saudi Arabia
e-mail: mkhurram@ksu.edu.sa

smart card based authentication faces various attacks. These attacks are based on the following security assumptions [22]: (i) An adversary is able to eavesdrop all the messages, which are transmitted in a cryptographic protocol; (ii) An adversary is able to modify, delete and resend all the messages, and can also reroute any message to any other principal in a cryptographic protocol; (iii) An adversary may be a legitimate participant or an outsider, or a combination of both; (iv) An adversary is able to obtain all the value of the session key that associate in any previously transmitted message. In-spite of above mentioned assumptions, an efficient and secure anonymous user authentication scheme for connected health care system should meet the following requirements: (a) Compatibility with TMIS; (b) Low computational and communication overhead with less storage requirement; (c) Efficient login and password change phase; (d) Resistance to different kinds of attacks; (e) User-friendly password change phase; (f) Mutual authentication and session key establishment.

Biometric keys (fingerprint, face, iris, hand geometry and palm-print, etc.) uniqueness property increase their application in authentication protocols. These keys helps to identify the correct user and enhance the security of authentication protocols. The biometric keys have some of the following advantages which have attracted significant research attention.

(1) Biometric keys need not to remember.
(2) Biometric keys are extremely difficult to forge.
(3) Biometric keys maintain uniqueness property.
(4) Biometric keys cannot be easily guessed.

The above mentioned advantages suggest that use of biometric keys in remote user authentication makes the remote user authentication schemes more secure and reliable compare to traditional password-based remote user authentication. Therefore, biometric-based remote user authentication schemes with a password have attracted significant research attention [23, 24]. In 2010, Li and Hwang [25] proposed a biometric based remote user authentication scheme in which user's biometrics key is used to verify the correctness of user. In 2011, Li et al. [26] pointed out that Li and Hwangs scheme does not withstand man-in-the-middle attack. They also proposed an improved biometrics-based remote user authentication scheme to remove the weaknesses of Li and Hwangs scheme. Moreover, their scheme presents session key agreement phase. In 2012, Truong et al. [27] pointed out that Li et al.'s scheme does not resist stolen verifier attack, man-in-the middle attack and replay attack. They also presented an improved scheme. However, their scheme does not provide efficient login and password change phase. Recently, Awasthi and Srivastava [28] proposed a biometric based authentication scheme for TMIS, which avoids the computation of time-consuming exponential operation and is best fit for low cost mobile devices.

In this paper, we briefly discuss Awasthi and Srivastava's scheme. We demonstrate how Awasthi and Srivastava's scheme fails to resist online and off-line password guessing attack. Additionally, we show that their scheme password change phase is inefficient to identify the incorrect input, which may cause denial of service attack. Further, we propose an improvement of Awasthi and Srivastava's biometric based authentication scheme for TMIS. Moreover, We present the security and performance analysis of the proposed scheme to support its claim.

Remaining paper is organized as follows: "Review of Awasthi and Srivastava's Scheme" section presents the brief review of Awasthi and Srivastava's scheme. "Preliminaries" section is a preliminary section which recalls the advantage of Biohashing and defines some notations. "Cryptanalysis of Awasthi and Srivastava's scheme" section points out the weaknesses of Awasthi and Srivastava's scheme. The proposed scheme is presented in "Proposed scheme" section. The security analysis of the proposed scheme is demonstrated in "Analysis" section. Finally, the conclusion is drawn in "Conclusion" section.

Preliminaries

Biohashing

The biometrics provides unique identification methods for the recognition on the basic feature of a human being and it works only when the person to be authenticated to be physically present for the authentication. In general, imprint biometric characteristics (face, fingerprint, palm-print) may not be exactly same at each time. The valid users' high false rejection resulting low false acceptation which is often occurs in the biometric systems' evaluation. The failing to identify authorized users significantly impacts on the usability of the system. On the contrary, the Biohashing can decrease denial of service access probability without losing the acceptation of false performance. In order to resolve the rejection of high false problem, Jin et al. [29] presented a iterated inner products based two-factor authenticator between user's fingerprint features and tokenized pseudo-random number. BioHashing technique is a mapping between biometric feature and user specific tokenized pseudo-random numbers [30]. In recent years, many improved BioHashing algorithms for human authentication have been present for more realistic scenario [31–35], which are a convenient mechanism to incorporate into small devices, such as mobile devices, smart card etc (Table 1).

Table 1 Notations that will be used throughout the paper

Notation	Descryption
U	User/Patient
S	A trustworthy medical system
E	Attacker/adversory
MD	Mobile device
ID_U	Unique identity of U
PW_U	Unique password of U
B_U	Personal biometrics of U
x	Master key of S
$h(\cdot)$	A collision free one-way chaotic hash function
$H(\cdot)$	Biohashing
$\oplus$	XOR operator
$\|\|$	String concatenation operation

Notations

Review of Awasthi and Srivastava's Scheme

Recently, Awasthi and Srivastava [28] proposed a biometric-based user authentication scheme for TMIS. Their scheme has following four phases:

1. Registration
2. Login
3. Authentication
4. Password change

In this section, we discuss Awasthi and Srivastava's scheme in brief. We try to adopts the same terminology as used in Awasthi and Srivastava's scheme.

Registration phase

A user U selects his/her identity ID_U and password PW_U, and chooses a random nonce N. He computes $PW_U \oplus N$ and encrypts $PW_U \oplus N$ using the public key PK_S of S and gets $E_{\mathsf{Pub(PK_S)}}(PW_U \oplus N)$, then submits ID_U and $E_{\mathsf{Pub(PK_S)}}(PW_U \oplus N)$ to the registration authority. User U also imprints his fingerprint impression $\gamma = (B_U \oplus N)$ at the sensor. Upon receiving registration request, the registration authority executes the following steps:

Step 1. Decrypt $E_{\mathsf{Pub(PK_S)}}(PW_U \oplus N)$ using the private key SK_S and achieve $PW_U \oplus N$.

Step 2. Compute $(PW_U \oplus N) \oplus (B_U \oplus N) = (PW_U \oplus B_U)$, $A_U = h(ID_U \oplus x)$ and $X_U = h(A_U)$. Then, compute $V_U = A_U \oplus h(PW_U \oplus B_U)$ where B_U is the extracted fingerprint template of the user.

Step 3 Personalize the information $ID_U, X_U, V_U, B_U, h(\cdot)$ of U and store them into U's mobile device.

Login phase

To start the login session, the user initiates the application and inputs his/her identity ID_U and password PW_U, and imprints his biometric B_U. If the biometric verification succeeds, then the mobile device executes the following steps:

Step 1. Compute $A_U = V_U \oplus h(PW_U \oplus B_U)$ and verify $X_U =? h(A_U)$. If the verification does not hold, it terminates the session. Otherwise, go to the next step.

Step 2. Compute $D_U = h(A_U \oplus T_U)$ where T_U is the current timestamp of the mobile device. Finally, U sends the login message $M_U =< ID_U, D_U, T_U >$ to the telecare system.

Authentication phase

Step 1. Upon receiving the message M_U at time T_S, S verifies the format of ID_U. If ID_U is invalid, it terminates the session. Otherwise, it verifies the freshness of timestamp using the condition $T_S - T_U \leq \Delta T$. If the condition holds, it runs step 2.

Step 2. S computes $A_U = h(ID_U \oplus x)$, then verifies $D_U =? h(A_U \oplus T_U)$. If verification holds, U is authenticated by S.

Step 3. S computes $D_S = h(A_U \oplus T_S)$, then sends the message $M_S =< D_S, T_S >$ to U.

Step 4. Upon receiving the message M_S, U checks that T_S is invalid or $T_S = T_U$. If any of the condition hold, he/she terminates the session. Otherwise, he/she verifies $D_S =? h(A_U \oplus T_S)$. If verification fails, it terminates the session. Otherwise, S is authenticated by U.

Password change phase

The valid user can change the password of his/her as follows:

Step 1. U inputs B_U with a request of password changes. After the success of authentication, the system asks old password PW_U and new password PW_{new}.

Step 2. U inputs old password PW_U and a new password PW_{new}.

Step 3. The system computes

$$V_{new} = V_U \oplus h(PW_U \oplus B_U) \oplus h(PW_{new} \oplus B_U)$$

then it updates V_U with V_{new}.

Cryptanalysis of Awasthi and Srivastava's scheme

In this section, we will analyze Awasthi and Srivastava's scheme and show the drawbacks of their scheme, which are based on the following assumptions:

- An adversary is able to extract the information from the smart card or mobile device [36–39].
- An adversary is able to eavesdrop all the messages between user and server, which are transmitted via public channel. Moreover, an adversary is able to modify, delete and resend all the messages, and can also reroute any message to any other entity [22, 40].
- An adversary may be a legitimate user or an outsider [22, 41].

Due to above mentioned assumptions, an adversary can achieve the parameters from the medical device $ID_U, X_U, V_U, B_U, h(\cdot)$ and can intercept and record the messages $< ID_U, D_U, T_U >$ and $< D_S, T_S >$, which are transmitted via public channel. With the help of these assumptions, an adversary can perform the following attacks successfully:

Undetectable on-line password guessing attack

In general, user selects a password, which he can easily remember as long and complex password is generally difficult to remember. In case, if a user selects a long and complex password and if he forget the password, he can no longer use the medical device or device. Additionally, if a user selects a long and complex password and stores it into some place or device, it increases the security risk. Therefore, to avoid these problems, user selects a password which he can easily remember. However, an adversary can try to guess the easy to memorable passwords. An efficient medical device based authentication protocol should resist password guessing attack. However, we identify that Awasthi and Srivastava's scheme does not withstand online password guessing attack. With the help of achieving values $\{ID_U, X_U, V_U, B_U, h(\cdot)\}$ from the medical device, an active adversary can successfully guess a valid user's password as follows:

Step 1. E guesses the password PW_U^* and computes $A_U^* = V_U \oplus h\left(PW_U^* \oplus B_U\right)$ and $D_U^* = h\left(A_U^* \oplus T_E\right)$, then sends $< ID_U, D_U^*, T_E >$ to the remote system where T_E is the current timestamp.

Step 2. Upon receiving the message at time T_S, remote system verifies the format of ID_U and freshness of timestamp. The verification succeeds as message includes user's original identity and current timestamp.

Step 3. Remote system computes $A_U = h(ID_U \oplus x)$, then verifies $D_U^* =? h(A_U \oplus T_E)$. If verification does not hold, it terminates the session. Otherwise, it replays with a valid message.

Step 4. If the session terminates, E repeats **Step 1** until succeeded. Otherwise, password guessing succeeds.

Off-line password guessing attack

An adversary can guess a legitimate user's password with the help of achieving values $\{ID_U, X_U, V_U, B_U, h(\cdot)\}$ from the medical device as follows:

Step 1. Guess the value PW_U^*, then compute $A_U^* = V_U \oplus h\left(PW_U^* \oplus B_U\right)$ and verify $X_U =? h(A_U^*)$.

Step 2. If the verification succeeds, considers PW_U^* as the user's password. Otherwise, he repeats **Step 1**.

Three factor authentication

In proposed scheme, only by knowing user's password, an adversary can generate a valid login message. Moreover, an adversary can establish authorized session with the help of leaked or guessed password to the server. This can be justified as follows:

- E can achieve U's secret value $A_U = h(ID_U \oplus x)$ with the help of leaked or guessed password PW_U and extracted biometric B_U and V_U from the device as $A_U = V_U \oplus h(PW_U \oplus B_U)$.
- Using achieved secret value A_U, E computes $D_E = h(A_U \oplus T_E)$ where T_E is the current timestamp. Then, E masquerades as a legitimate user and sends the login message $M_E =< ID_U, D_E, T_E >$ to the remote system.
- Upon receiving the message M_E at time T_E', S verifies the format of ID_U and freshness of timestamp. The verification succeeds as message includes user's original identity and current timestamp.
- S computes $A_U = h(ID_U \oplus x)$, then verifies $D_E = ?h(A_U \oplus T_E)$. Obviously, the verification will hold due to correct secret value A_U used in D_E by E. In this way, E authenticates itself to S as a legal user.

Biometric based authentication scheme supports three-factor authentication where leakage of one authentication parameter does not enable to an adversary to successfully login to the system. However, by knowing user's password, an adversary can successfully login to the server in Awasthi and Srivastava's scheme. This shows that adoption of biometric keys does not enhance security of authentication scheme. In other words, Awasthi and Srivastava's scheme does not achieve three-factor authentication.

Inefficient password change phase

In Awasthi and Srivastava's scheme, mobile device executes the password change after the successful verification of fingerprint biometric without verifying the correctness of the password. However, a user may enter wrong password as human may sometimes forget the password or commit mistake or user can use one account's password into another account. This may cause the denial of service attack where a user will no longer be able to login to the server using the same device. To change the password, user U inputs B_U then the mobile device verifies the correctness of B_U. If verification holds, it asks for old password and new password. Let a user input the wrong old password PW_U^* instead of PW_U, *i.e.*, $PW_U^* \neq PW_U$, then the password change phase executes as follows:

– U inputs incorrect password PW_U^* and new password PW_{new}.
– Without verifying the correctness of the old password, the system computes

$$\begin{aligned} V_{new} &= V_U \oplus h(PW_U^* \oplus B_U) \oplus h(PW_{new} \oplus B_U) \\ &= A_U \oplus h(PW_U \oplus B_U) \oplus h(PW_U^* \oplus B_U) \oplus h(PW_{new} \oplus B_U) \\ &\neq A_U \oplus h(PW_{new} \oplus B_U),\ as\ PW_U^* \neq PW_U \end{aligned}$$

and updates V_U with V_{new}.

The above discussion concludes that the scheme is inefficient to detect wrong password, this will cause denial of service permanently where a legitimate user can never establish an authorized session with the server using the same mobile device. If a user has updated his password using wrong password instead of old correct password, then the user will face denial of service as follows:

- User inputs updated password PW_{new} and identity ID_U, and imprints his fingerprint biometric B_U. The biometric verification holds as user himself imprints his fingerprint.
- Once the biometric verification succeeds, user's device computes A_U^* as follows:

$$\begin{aligned} A_U^* &= V_{new} \oplus h(PW_{new} \oplus B_U) \\ &= A_U \oplus h(PW_U \oplus B_U) \oplus h(PW_U^* \oplus B_U) \oplus h(PW_{new} \oplus B_U) \\ &\quad \oplus h(PW_{new} \oplus B_U) \\ &= A_U \oplus h(PW_U \oplus B_U) \oplus h(PW_U^* \oplus B_U) \\ &\neq A_U,\ as\ PW_U^* \neq PW_U \end{aligned}$$

- User,s device computes $D_U^* = h(A_U^* \oplus T_U)$ and sends $< ID_U, D_U^*, T_U >$ to the remote system, where T_U is the current timestamp.
- Upon getting the message at time T_U', medical system verifies format of ID_U. The verification holds as message includes user's original identity. It also verifies the freshness of timestamp using the condition $T_U' - T_U \leq \Delta T$. The verification succeeds as user used current timestamp.
- System computes $A_U = h(ID_U \oplus x)$, then verifies $D_U^* =?\ h(A_U \oplus T_U)$. The verification does not hold as $D_U^* \neq h(A_U^* \oplus T_U)$, due to $A_U^* \neq A_U$. Thus the system S terminates the session.

It is clear from the above discussion that user cannot establish an authorized session with the server after updating the password wrongly.

Proposed scheme

We modify the Awasthi and Srivastava's scheme to remove its drawbacks. The modified scheme comprises the similar phases like Awasthi and Srivastava's scheme. In proposed schemes, the registration, login, authentication and password change phase work as follows:

Registration phase

A new user U needs to be registered in the Telecare medicine information system to access the resources. In this regard, a user needs to submit his registration request with identity, password and biometric information to the system. Upon receiving the information, the system verifies the registration details of user and registers him as an authorized. This process executes as follows:

Step 1. User U selects his/her identity ID_U and password PW_U of his choice, and chooses a random nonce N. He imprints his/her fingerprint B_U and computes $PW_U \oplus N$ and $H(B_U) \oplus N$. He submits the registration request with ID_U, $PW_U \oplus N$ and $H(B_U) \oplus N$ to S via secure channel.

Step 2. Upon receiving registration request, S verifies the registration of ID_U. If ID_U is registered with some other user, it asks for a new identity. Otherwise, S computes $(PW_U \oplus N) \oplus (H(B_U) \oplus N) = PW_U \oplus H(B_U)$ and $A_U = h(ID_U||x||T_R)$ using its master key x, where T_R is the registration time.

Step 3. S also computes $X_U = h(A_U)$ and $V_U = A_U \oplus (PW_U \oplus H(B_U))$ and then maintains the record of registration time T_R corresponding to user identity ID_U.

Step 4. S personalizes the information ID_U, X_U, V_U, $h(\cdot)$, $H(\cdot)$ for U and stores these personalized security parameters in the user's mobile device (Fig. 1).

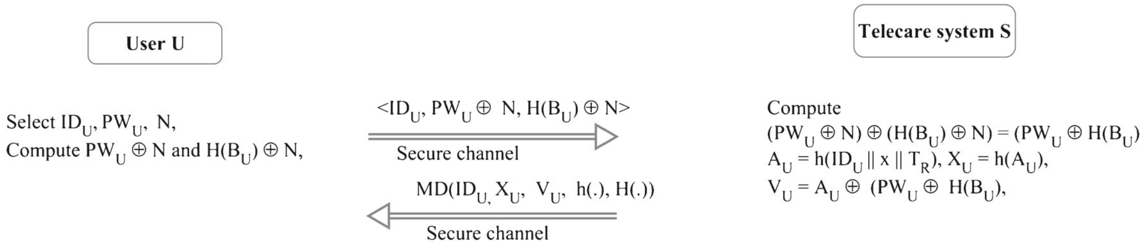
User U
Telecare system S
Select ID_U, PW_U, N,
Compute $PW_U \oplus N$ and $H(B_U) \oplus N$,
$<ID_U, PW_U \oplus N, H(B_U) \oplus N>$
Secure channel
$MD(ID_U, X_U, V_U, h(.), H(.))$
Secure channel
Compute
$(PW_U \oplus N) \oplus (H(B_U) \oplus N) = (PW_U \oplus H(B_U)$
$A_U = h(ID_U \| x \| T_R)$, $X_U = h(A_U)$,
$V_U = A_U \oplus (PW_U \oplus H(B_U)$,

Fig. 1 The pictorial representation of registration phase

Login phase

When a user wishes to access the Telecare system, he needs to successfully complete the login and authentication phase. With the help of his/her mobile device, a user executes the login session as follows:

Step 1. U first initiates the application on the device and then inputs his/her password PW_U. He imprints his/her fingerprint biometric B_U.

Step 2. Mobile device achieves $A_U = V_U \oplus (PW_U \oplus H(B_U))$ and verifies $X_U = ?\ h(A_U)$. If the verification does not hold, it terminates the session. Otherwise, it runs step 3.

Step 3. Mobile device computes $D_U = h(A_U||T_U)$, where T_U is the current timestamp of the mobile device. Finally, U sends the login message $M_U =< ID_U, D_U, T_U >$ to the Telecare system.

Authentication phase

In authentication phase, both user and server verify the authenticity of each other.

Step 1. Upon receiving the message M_U at time T'_U, S verifies the freshness of timestamp using the condition $T'_U - T_U \leq \Delta T$, where ΔT is the valid time delay in message transmission. If the condition holds,it searches ID_U in its database. If ID_U is in the database, it achieves user's registration time T_R and computes $A_U = h(ID_U||x||T_R)$, then verifies $D_U = ?\ h(A_U||T_U)$. If verification holds, U is authenticated by S.

Step 2. S computes $D_S = h(D_U||A_U||T_S)$, then sends the message $M_S =< D_S, T_S >$ to U at time T_S.

Step 3. Upon receiving the message M_S, U verifies the condition $T_S - T_U < \Delta T$. If verification does not hold, he/she terminates the session. Otherwise, he/she verifies $D_S = ?\ h(D_U||A_U||T_S)$. If verification fails, he/she terminates the session. Otherwise, S is authenticated by U (Fig. 2).

Password change phase

To change the password of device, a user first selects a new password and then he can change the password without server assistance as follows:

Step 1. U inputs passwords PW_U and imprints his/her fingerprint B_U with a request of password change to the mobile device.

Step 2. Mobile device computes $H(B_U)$ and $A_U = V_U \oplus (PW_U \oplus H(B_U))$, then verifies $X_U =?\ h(A_U)$. If the verification does not hold, it terminates the session. Otherwise, it asks for a new password from the user U. Then, U enters a new password PW_{new}(Fig. 3).

Step 3. Mobile device computes

$$(V_U)_{new} = V_U \oplus (PW_U \oplus H(B_U)) \oplus (PW_{new} \oplus H(B_U))$$

then it updates V_U with $(V_U)_{new}$.

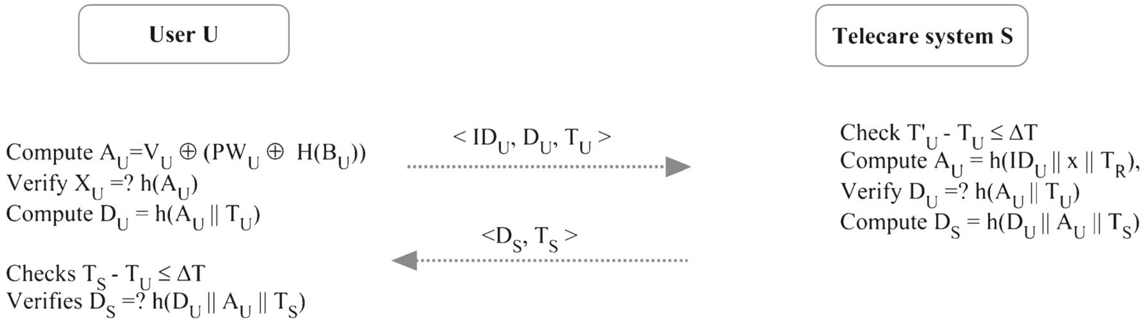
User U
Telecare system S
Compute A_U=$V_U \oplus (PW_U \oplus H(B_U))$
Verify X_U =? $h(A_U)$
Compute $D_U = h(A_U \| T_U)$
$< ID_U, D_U, T_U >$
$<D_S, T_S >$
Checks $T_S - T_U \leq \Delta T$
Verifies D_S =? $h(D_U \| A_U \| T_S)$
Check $T'_U - T_U \leq \Delta T$
Compute $A_U = h(ID_U \| x \| T_R)$,
Verify D_U =? $h(A_U \| T_U)$
Compute $D_S = h(D_U \| A_U \| T_S)$

Fig. 2 The pictorial representation of login and authentication phase

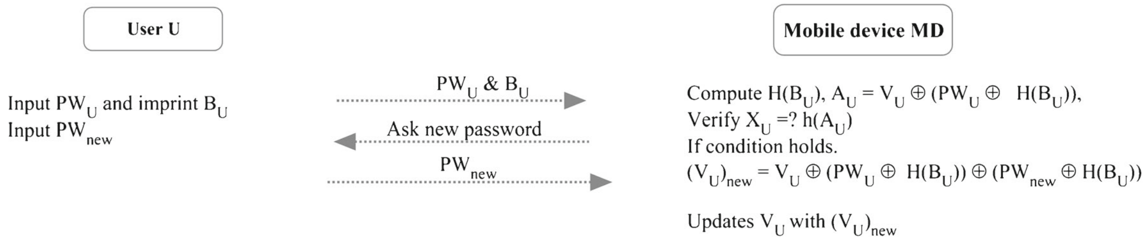
User U
Mobile device MD
Input PW_U and imprint B_U
Input PW_{new}
PW_U & B_U
Ask new password
PW_{new}
Compute $H(B_U)$, $A_U = V_U \oplus (PW_U \oplus H(B_U))$,
Verify X_U =? $h(A_U)$
If condition holds.
$(V_U)_{new} = V_U \oplus (PW_U \oplus H(B_U)) \oplus (PW_{new} \oplus H(B_U))$
Updates V_U with $(V_U)_{new}$

Fig. 3 The pictorial representation of password change phase

Analysis

Security analysis

The detailed security analysis of the proposed scheme to verify how the scheme satisfies the security requirements is as follows:

Insider attack

A malicious insider in server's system may try to achieve user's secrets, such as the user's password. However, in the proposed scheme, the user does not submit his/her password PW_U and biometrics B_U in its original form, *i.e.,* user submits $PW_U \oplus N$ and $B_U \oplus N$ instead of PW_U and B_U to the registration authority, where N is a random number. Therefore, an inside can only achieve $PW_U \oplus N$ and $B_U \oplus N$, and can at most compute $PW_U \oplus B_U$. Since N and B_U both are unknown to the insider. Therefore, it will be hard to achieve PW_U form $PW_U \oplus N$ or $PW_U \oplus B_U$. This shows that the proposed scheme resists insider attack.

Stolen device attack

Suppose an attacker has stolen user's mobile device. Then, the attacker may wish to use the stolen device to login to the Telecare system. Although the attacker cannot be authenticated successfully by the medical server because the attacker cannot compute the valid login message. This is clear from the following facts:

- The attacker can retrieve the information $\{ID_U, V_U, X_U\}$ from the stolen mobile device. However, an attacker cannot achieve $A_U = h(ID_U||x||T_R)$ from $V_U = A_U \oplus (PW_U \oplus H(B_U))$ as both parameters PW_U and B_U are unknown to the attacker.
- The attacker cannot construct $A_U = h(ID_U||x||T_R)$ as both x and T_R are unknown to the attacker.

The above discussion shows that, the proposed scheme withstands stolen mobile device attack.

On-line password guessing attack

An active adversary can try to perform on-line password guessing attack using the information $ID_U, X_U = h(A_U), V_U = A_U \oplus (PW_U \oplus H(B_U))$ and $D_U = h(A_U||T_U)$ because of the following facts:

- Let E guesses the password PW^*.
- To verify the guessed password PW^*, E tries to generate a valid login message $< ID_U, D_U, T_U >$, which is equivalent to achieve A_U from $V_U = A_U \oplus (PW_U \oplus H(B_U))$ using guessed password PW^*. However, A_U cannot be achieved from V_U even by using user's original password PW_U as A_U is protected with the password along with biometric where biometric is a unique identifier and is difficult to guess.

Off-line password guessing attack

An adversary can try to guess a user's password. However, he cannot verify the guessed password correctly with the achieved information $ID_U, X_U = h(A_U), V_U = A_U \oplus (PW_U \oplus H(B_U))$ and $D_U = h(A_U||T_U)$ because of the following facts:

- Let E guesses the password PW^*.
- To verify the guessed password PW^* with $X_U = h(A_U)$ is equivalent to achieve A_U from $V_U = A_U \oplus (PW_U \oplus H(B_U))$. However, to achieve A_U from $V_U = A_U \oplus (PW_U \oplus H(B_U))$, requires user's fingerprint biometric B_U. Since, no third party can imprint the biometric information of a user, E can not achieve A_U from V_U. Therefore, E cannot successfully guess password with X_U.
- To verify the guessed password PW^* with $D_U = h(A_U||T_U)$ is also equivalent to achieve A_U from $V_U = A_U \oplus (PW_U \oplus H(B_U))$. Although it is not feasible to compute A_U from V_U as discuss above.

Replay attack

The timestamp is considered to be the countermeasure to resist the replay attack. The proposed scheme adopts timestamp as a counter measure to resist replay attack. However, an attacker E can try to perform replay attack, which will not succeed due to following facts:

- E replays the previously transmitted message $< ID_U, D_U, T_U >$. Since, the remote system identifies the freshness of message by verifying the freshness of timestamp. Therefore, remote system can easily identify replay message.
- E replaces the message $< ID_U, D_U, T_U >$ with $< ID_U, D_U, T_E >$, and sends $< ID_U, D_U, T_E >$ to the remote system, where T_E is the current timestamp. When a remote system verifies the freshness of timestamp, the verification holds as an adversary replaces the old timestamp with the current timestamp. However, when the remote system verifies $D_U =? h(A_U||T_E)$, the verification does not hold as $D_U = h(A_U||T_U)$ and $T_U \neq T_E$.
- E can try to replace the message $< ID_U, D_U, T_U >$ with $< ID_U, D_E, T_E >$, where $D_E = h(A_U||T_E)$. However, E cannot compute D_E as A_U is unknown to E.

User impersonation attack

In user impersonation attack, an attacker masquerades as a legal user to server. To succeed the user impersonation attack, an attacker has to generate a valid login message $< ID_U, D_E, T_E >$, where $D_E = h(A_U||T_E)$ and T_E is the current timestamp. However, to compute $D_E = h(A_U||T_E)$ is equivalent to achieve A_U from $V_U = A_U \oplus (PW_U \oplus H(B_U))$. However, to achieve A_U from V_U user's password along with fingerprint are needed. Since, the attacker can not imprint user's fingerprint and unknown with the user's password. Therefore, an attacker cannot generate a valid login message. This shows that the proposed scheme resists user impersonation attack.

Server impersonation attack

The proposed scheme resists server impersonation attack as follows:

- User computes the login message and sends $< ID_U, D_U, T_U >$ to the remote system.
- An adversary intercepts U's messages and tries to respond with a valid message $< D_S, T_S >$, where $D_S = h(D_U||A_U||T_S)$. However, to compute $D_S = h(D_U||A_U||T_S)$, user's secret key A_U is needed, which is unknown to E. To compute A_U from $V_U = A_U \oplus (PW_U \oplus H(B_U))$ requires PW_U and B_U. Since both the values PW_U and BW_U are secret, an adversary cannot masquerade as the remote system. Moreover, to compute $A_U = h(ID_U||x||T_R)$, server's master key x is needed which is also a secret. This shows that the proposed scheme resists server impersonation attack.

Mutual authentication

In mutual authentication mechanism, both user and server verify the authenticity of each other. In the proposed scheme, user and server both authenticate each other. To achieve this, user and server exchange $D_U = h(A_U||T_U)$ and $D_S = h(D_U||A_U||T_S)$, where T_U and T_S are the current timestamps of U and S, respectively. To forge user or server, an attacker has to construct D_U or D_S, respectively. However, to construct D_U or D_S is equivalent to achieve user's secret key A_U, which can compute only user and server. Since an adversary can not forge user or server. Therefore, the server and user can correctly identify the correctness of each other.

Efficient login phase

In the proposed scheme, mobile device can quickly detect incorrect login input as follows:

Case-1 If a user password is leaked or guessed by an adversary and wish to fraud in fingerprint imprint, *i.e.*, if the mobile device receives inputs including correct password PW_U and imprints of wrong fingerprint biometric B_U^*, it can quickly detect and identify as follows:

- Mobile device computes $H(B_U^*)$ and then $A_U^* = V_U \oplus (PW_U \oplus H(B_U^*))$. It is clear that $A_U \neq A_U^*$ as $B_U^* \neq B_U$.
- When the mobile device verifies $X_U = ? h(A_U^*)$, the verification does not hold as $X_U = h(A_U) \neq h(A_U^*)$.

Case-2 If a user inputs incorrect password PW_U^* and imprints his/her correct fingerprint biometric B_U then

- Mobile device computes $H(B_U)$ and then $A_U^* = V_U \oplus (PW_U^* \oplus H(B_U))$. It is clear that $A_U \neq A_U^*$ as $PW_U^* \neq PW_U$.
- When the mobile device verifies $X_U = ? h(A_U^*)$, the verification does not hold as $X_U = h(A_U) \neq h(A_U^*)$.

Case-3 If a user inputs incorrect password PW_U^* and imprints of wrong fingerprint biometric B_U^*

Table 2 Security attributes comparison of the proposed scheme with other relevant biometric based authentication schemes

Security attributes \ Schemes	[25]	[26]	[27]	[42]	[28]	Proposed
Insider Attack	×	√	√	×	√	√
Stolen verifier attack	√	×	√	√	√	√
User impersonation attack	×	√	√	√	√	√
Stolen mobile device attack	√	√	√	√	√	√
Replay attack	√	√	√	√	√	√
Denial of service attack	√	√	√	√	×	√
Off-line password guessing attack	√	√	√	×	×	√
Mutual authentication	×	√	√	√	√	√
User-friendly password selection	√	√	√	√	√	√
Efficient login	×	×	×	×	√	√
Efficient password change	×	×	×	×	×	√
Three factor authentication	×	×	√	×	×	√

– Mobile device computes $H(B_U^*)$ and then $A_U^* = V_U \oplus (PW_U^* \oplus H(B_U^*))$. It is clear that $A_U \neq A_U^*$ as $PW_U^* \neq PW_U$ and $H(B_U^*) \neq H(B_U)$.

– When the mobile device verifies $X_U \; =?\; h(A_U^*)$, the verification does not hold as $X_U = h(A_U) \neq h(A_U^*)$.

In all three cases, mobile device can efficiently detect the incorrect input and can terminate the session. This shows that the proposed scheme has efficient login phase.

User-friendly and efficient password changes phase

In the proposed scheme, the user can change his/her password without remote system assistance anytime and anywhere. Moreover, the user's device verifies the correctness of inputs with the condition $X_U =? \; h(A_U)$ as demonstrated in login phase, *i.e.*, device performs the same verification test in password change phase as it performs in the login phase. Therefore, efficiency of password change phase is equivalent to the efficiency of the login phase in incorrect input detection. Since the login phase is efficient, therefore password change phase is also efficient.

Three factor-authentication

As it is clear from the above discussion that in order to successfully login to the remote system, a user has to compute D_U in the proposed scheme. However, to compute D_U, user's secret key A_U is needed. To achieve A_U from V_U, the correct password PW_U and fingerprint B_U are needed. This shows that to generate a valid login message or to access the mobile device both the security parameters, password and biometric are needed. This shows that the proposed scheme achieves three-factor authentication.

We will also compare the security attributes of our scheme with Li and Hwang's [25], Li et al.'s [26], Troung et al.'s [27], Chang's et al.'s [42] and Awasthi and Srivastava's [28] schemes in Table 2. If the scheme prevents attack or satisfies the property, the symbol '√' is used and if it fails to prevent attack or does not satisfy the attribute, the symbol × is used.

Performance Analysis

In general, the medical devices have limited storage space and limited computation power. Therefore, the

Table 3 Computation cost comparison of the proposed scheme with some relevant schemes

Phases\ Schemes	[25]	[26]	[27]	[42]	[28]	Proposed
Registration	$3T_h$	$4T_h$	$5T_h$	$4T_h$	$2T_{PK} + 3T_h$	$3T_h$
Login	$2T_h$	$4T_h$	$5T_h$	$3T_h$	$3T_h$	$3T_h$
Authentication	$5T_h$	$7T_h$	$9T_h$	$7T_h$	$4T_h$	$4T_h$
Password Change	$3T_h$	$4T_h$	$4T_h$	$3T_h$	$2T_h$	$2T_h$
Total	$13T_h$	$19T_h$	$23T_h$	$17T_h$	$2T_{PK} + 12T_h$	$12T_h$

authentication protocol must give priority to the efficiency due to resource constraints in mobile device [43]. In this section, we show the efficiency analysis of proposed schemes with some relevant schemes in Table 3, where T_{PK}, T_h and T_X denote the time complexity of public key encryption/decryption, hash function and XOR operation, respectively. It is stated $T_{PK} >> T_h >> T_X$ in [44, 45]. Since the computation overhead of XOR is relatively very less, we are ignoring the computation of XOR operation in our comparison.

Conclusion

The proposed article presents a brief review of Awasthi and Srivastava's scheme and points out the drawbacks of their scheme. The analysis shows that Awasthi and Srivastava's scheme does not fulfill their claims as it suffers on-line and off-line password guessing attack. We also demonstrated that their scheme does not achieve three-factor authentication. Moreover, we identified that inefficient password change phase in their scheme causes denial of service attack. Further, we have presented an improved biometric based remote authentication scheme for TMIS to remove the flaws of Awasthi and Srivastava's scheme. The security and performance analysis show that the proposed scheme resists all kinds of attacks and provides efficient password change phase where incorrect login can be quickly detected.

Conflict of interests The authors declare that they have no conflict of interest.

References

1. Latré, B., Braem, B., Moerman, I., Blondia, C., Demeester, P., A survey on wireless body area networks. *Wirel. Netw.* 17(1):1-18, 2011.
2. Khan, M. K., Kumari, S., An authentication scheme for secure access to healthcare services. *J. Med. Syst.* 37(4):1-12, 2013.
3. Srivastava, K., Awasthi, A. K.,Mittal, R., A review on remote user authentication schemes using smart cards. In: Quality, Reliability, Security and Robustness in Heterogeneous Networks. Springer (2013) 729–749.
4. Cao, T., Zhai, J., Improved dynamic id-based authentication scheme for telecare medical information systems. *J. Med. Syst.* 37(2):1-7, 2013.
5. 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.
6. Chen, Y. Y., Lu, J. C., Jan, J. K., A secure ehr system based on hybrid clouds. *J. Med. Syst.* 36(5):3375–3384, 2012.
7. 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(5):1–17, 2013.
8. Debiao, H., Jianhua, C., Rui, Z., A more secure authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(3):1989–1995, 2012.
9. Guo, R., Wen, Q., Shi, H., Jin, Z., Zhang, H., An efficient and provably-secure certificateless public key encryption scheme for telecare medicine information systems. *J. Med. Syst.* 37(5):1–11, 2013.
10. Jiang, Q., Ma, J., Ma, Z., Li, G., A privacy enhanced authentication scheme for telecare medical information systems. *J. Med. Syst.* 37(1):1-8, 2013.
11. 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(2):1–18, 2014.
12. Kumari, S., Khan, M. K., Kumar, R., Cryptanalysis and improvement of a privacy enhanced scheme for telecare medical information systems. *J. Med. Syst.* 37(4):1–11, 2013.
13. Lee, T. F. An efficient chaotic maps-based authentication and key agreement scheme using smartcards for telecare medicine information systems. *J. Med. Syst.* 37(6):1–9, 2013.
14. Lee, T. F., Liu, C. M., A secure smart-card based authentication and key agreement scheme for telecare medicine information systems. *J. Med. Syst.* 37(3):1–8, 2013.
15. Lin, S. S., Hung, M. H., Tsai, C .L., Chou, L. P., Development of an ease-of-use remote healthcare system architecture using rfid and networking technologies. *J. Med. Syst.* 36(6):3605–3619, 2012.
16. Pu, Q., Wang, J., Zhao, R., Strong authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(4):2609–2619, 2012
17. Siddiqui, Z., Abdullah, A. H., Khan, M. K., Alghamdi, A. S., Smart environment as a service: Three factor cloud based user authentication for telecare medical information system. *J. Med. Syst.* 38(1):1–14, 2014.
18. 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.
19. Xie, Q., Zhang, J., Dong, N., Robust anonymous authentication scheme for telecare medical information systems. *J. med. syst.* 37(2):1–8, 2013.
20. 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.* 38(1):1–7, 2014.
21. Zhu, Z., An efficient authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(6):3833–3838, 2012.
22. Boyd, C., and Mathuria, A., Protocols for authentication and key establishment. Springer (2003)
23. Leng, L., Teoh, A. B. J., Li,M., Khan, M. K., A remote cancelable palmprint authentication proto- col based on multi-directional two-dimensional palmphasor-fusion. Secur. Commun. Networks, doi:10.1002/sec.900, 2013.
24. Bowyer, K. W., Hollingsworth, K. P., Flynn, P. J., A survey of iris biometrics research: 2008–2010. In: Handbook of iris recognition. Springer (2013) 15–54
25. Li, C. T., Hwang, M. S., An efficient biometrics-based remote user authentication scheme using smart cards. *J. Netw. Comput. Appl.* 33(1):1–5, 2010.
26. Li, X., Niu, J. W., Ma, J., Wang, W. D., Liu, C. L., Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards. J. *Netw. Comput. Appl.* 34(1):73–79, 2011.
27. Truong, T. T., Tran,M. T., Duong, A. D., Robust biometrics based remote user authentication scheme using smart cards. In: *15th*

IEEE International Conference on Network-Based Information Systems (NBiS'2012), pp. 384–391, 2012

28. 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.
29. Jin, A. T. B., Ling, D. N. C., Goh, A., Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern recognit.* 37(11):2245–2255, 2004.
30. Zhou, X., and Kalker, T., On the security of biohashing. In: IS&T/SPIE Electronic Imaging, International Society for Optics and Photonics. pp. 75410–75410, 2010.
31. Leng, L., and Zhang, J., Palmhash code vs. palmphasor code. *Neurocomput.* 108:1–12, 2013.
32. Belguechi, R., Rosenberger, C., Ait-Aoudia, S.: Biohashing for securing minutiae template. In: *20th IEEE International Conference on Pattern Recognition (ICPR'2010)*, pp. 1168–1171, 2010.
33. Lumini, A., and Nanni, L., An improved biohashing for human authentication. *Pattern Recognit.* 40(3):1057–1065, 2007.
34. Yang, C.: Integration of biometrics and pin pad on smart card. PhD thesis, University of Newcastle Upon Tyne 2011.
35. Leng, L., Zhang, J., Khan, M. K., Chen, X., Ji, M., Alghathbar, K., Cancelable palmcode generated from randomized gabor filters for palmprint template protection. *Sci. Res. Ess.* 6(4):784–792, 2011.
36. Brier, E., Clavier, C., Olivier, F., Correlation power analysis with a leakage model. In: Cryptographic Hardware and Embedded Systems (CHES'2004), pp. 16–29. Springer, 2004.
37. Eisenbarth, T., Kasper, T., Moradi, A., Paar, C., Salmasizadeh, M., Shalmani, M. T. M., On the power of power analysis in the real world: A complete break of the keeloq code hopping scheme. In: Advances in Cryptology-(CRYPTO'2008), pp. 203–220. Springer, 2008.
38. Kocher, P., Jaffe, J., Jun, B., Differential power analysis. In: Advances in Cryptology (CRYPTO'99), pp. 388–397. Springer, 1999.
39. Messerges, T. S., Dabbish, E. A., Sloan, R. H., Examining smart-card security under the threat of power analysis attacks. *IEEE Trans. Consum. Electron.* 51(5):541–552, 2002
40. Xu, J., Zhu, W. T., Feng, D. G., An improved smart card based password authentication scheme with provable security. *Comput. Stand. Interfaces* 31(4):723–728, 2009.
41. Yang, C. C., Yang, H. W., Wang, R. C., Cryptanalysis of security enhancement for the timestampbased password authentication scheme using smart cards. *IEEE Trans. Consum. Electron.* 50(2):578–579, 2004.
42. Chang, Y. F., Yu, S. H., Shiao, D. R., A uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care. *J. Med. Syst.* 37(2):1–9, 2013
43. Liao, Y. P., and Wang, S. S., A secure dynamic id based remote user authentication scheme for multi-server environment. *Comput. Stand. Interfaces* 31(1):24–29, 2009
44. Potlapally, N. R., Ravi, S., Raghunathan, A., Jha, N. K., A study of the energy consumption characteristics of cryptographic algorithms and security protocols. *IEEE Trans. Mob. Comput.* 5(2):128–143, 2006
45. Wong, D. S., Fuentes, H. H., Chan, A. H., The performance measurement of cryptographic primitives on palm devices. In: Proceedings 17th IEEE Annual Computer Security Applications Conference (ACSAC'2001), pp. 92–101, 2001.