J Med Syst (2014) 38:24
DOI 10.1007/s10916-014-0024-2

PATIENT FACING SYSTEMS

Cryptanalysis and Improvement of Yan et al.'s Biometric-Based Authentication Scheme for Telecare Medicine Information Systems

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

Received: 17 November 2013 / Accepted: 4 March 2014 / Published online: 1 June 2014
© Springer Science+Business Media New York 2014

Abstract Remote user authentication is desirable for a Telecare Medicine Information System (TMIS) for the safety, security and integrity of transmitted data over the public channel. In 2013, Tan presented a biometric based remote user authentication scheme and claimed that his scheme is secure. Recently, Yan et al. demonstrated some drawbacks in Tan's scheme and proposed an improved scheme to erase the drawbacks of Tan's scheme. We analyze Yan et al.'s scheme and identify that their scheme is vulnerable to off-line password guessing attack, and does not protect anonymity. Moreover, in their scheme, login and password change phases are inefficient to identify the correctness of input where inefficiency in password change phase can cause denial of service attack. Further, we design an improved scheme for TMIS with the aim to eliminate the drawbacks of Yan et al.'s scheme.

Keywords Telecare medicine information system · Smart card · Remote user authentication · Biometric · Password

This article is part of the Topical Collection on *Patient Facing Systems*

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

D. Mishra
e-mail: dheerendra@maths.iitkgp.ernet.in

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

S. Kumari
Department of Mathematics, Agra College, Agra, Dr. B. R. A. University, Agra, Uttar Pradesh, India

S. Kumari
e-mail: saryusiirohi@gmail.com

M. K. Khan
Center of Excellence in Information Assurance, King Saud University, Riyadh, Kingdom of Saudi Arabia

M. K. Khan
e-mail: mkhurram@ksu.edu.sa

Introduction

The rapid development in network and communication technology has presented a scalable platform for Telecare Medicine Information System (TMIS). The communication between the user and server is always a subject of security and privacy risk in TMIS as user accesses remote server via public channel and an adversary is considered to be enough powerful to perform various attacks. Thus the secure and efficient authenticated key agreement schemes should be adopted to ensure security and integrity of transmitting data [1]. The smart card based authentication scheme provides efficient solution for remote user authentication [2, 3]. In recent times, many password based authentication schemes have been proposed for TMIS [4–11]. These schemes try to provide two factor authentication.

The password cannot be considered as a unique identity identifier and it's needed to be remembered. Moreover, possibility of password guessing attack is also a concern. However, biometrics cannot be lost or forgotten, have the merits of uniqueness and need not be remembered; but they can be compromised [12, 13]. Additionally, these biometric keys are not easy to guess [14, 15]. Due to these advantages, the biometrics based authentication schemes present efficient solution to mutually authenticate and session key agreement. In 2013, Tan [16] presented a biometric based remote user authentication scheme for the Telecare medical information system. In Tan's scheme, a remote user and server can mutually authenticate each other and draw a session key. Moreover, the Tan's scheme presents a user-friendly password and biometric update phase where a user can change his password and biometric keys without server assistance. Recently, Yan et al.'s [17] pointed out that Tan's scheme is vulnerable to denial-of-service attack. Further, they proposed an improved scheme to eliminate the drawbacks of Tan's scheme. Their scheme also preserves all the merits of Tan's scheme.

In this article, we analyze the Yan et al.'s biometrics based remote user authentication scheme for TMIS. We show that Yan et al.'s scheme login phase is inefficient such that the smart card executes the login session in-spite of incorrect input. The inefficiency of the login phase in incorrect input detection causes extra communication and computation overhead. Yan et al.'s password and biometrics update phase is also inefficient to detect incorrect input, which causes denial of service attack in case of wrong password input. Yan et al.'s scheme does not withstand password guessing attacks. Furthermore, we present a modified scheme which overcomes the weaknesses of Yan et al.'s scheme and preserves its merits.

The remaining part of the article is organized as follows: Section "Review of Yan et al.'s scheme" presents a brief review of Yan et al.'s scheme. Section "Preliminaries" shows some notations and recall the definition of biohasing. Section "Weaknesses of Yan et al.'s scheme" demonstrates the weaknesses of Yan et al.'s scheme. The proposed scheme and its analysis are presented in section "Proposed scheme" and section "Analysis", respectively. The comparison is shown in section "Comparison". The conclusion is drawn in section "Conclusion".

Preliminaries

Biohashing

The biometrics provides unique identification methods for the recognition of a human being based on his/her unique biometric characteristic; it works only when the person to be authenticated is physically presented for the authentication. In general, imprint biometric characteristics (face, fingerprint, palmprint) may not be exactly same at each time. Therefore, high false rejection of valid users result in low false acceptation, it often occurs in the verification through biometric systems. The failing to identify authorized users significantly impacts on the usability of the system. On the contrary, the Biohashing can reduce the probability of denial of access without losing the false acceptation performance. In order to resolve the high false rejection problem, Jin et al. [18] presented a two-factor authenticator based on iterated inner products between tokenized pseudo-random number and the user specific fingerprint features. To achieve this, a set of user specific compact codes can be created that is called BioHash code. BioHashing technique is a mapping biometric feature randomly onto binary strings with user specific tokenized pseudo-random numbers. In recent years, many improved BioHashing algorithms for human authentication have been presented for more realistic scenario [19–21], which are a convenient mechanism to incorporate into small devices, such as mobile devices, smartcard etc.

Table 1 Meaning of symbols used throughout the paper

Notation	Descryption
U_i	User i
S	A trustworthy medical server
E	Adversary
ID_i	Identity of user i
PW_i	Password of user i
B_i	Biometrics of user i
x	Master key of S
$\text{Sym.Enc}_{(x)}(M)$	Symmetric key encryption of message M using key x
$\text{Sym.Dec}_{(x)}(M)$	Symmetric key decryption of message M using key x
$h(\cdot)$	A collision free one-way hash function
$H(\cdot)$	Biohash function
$\oplus$	XOR
$\|\|$	String concatenation operation

Notations

In Table 1, we will define all the notations which are used throughout the paper.

Review of Yan et al.'s scheme

In 2013, Yan et al. [17] proposed an improvement of Tan's [16] biometrics-based authentication scheme for TMIS. This comprises of four phases similar to Tan's scheme, which are as follows: registration, login, authentication and key agreement, and password change . We will briefly discuss all the phases of Yan et al.'s scheme. This discussion comprises most of the facts as it is as presented in Yan et al.'s article. The brief description of Yan et al.'s scheme is as follows:

Registration phase

A new user U_i can register and achieve personalized smart card as follows:

Step 1. U_i selects his identity ID_i and password PW_i. U_i imprint his biometrics B_i. U_i also generates a random number N_i and computes $W = h(ID_i||PW_i||B_i||N_i)$. U_i submits ID_i and W to S via secure channel.

Step 2. S computes $X_i = h(ID_i||x)$ and $Y_i = X_i \oplus h(W)$, where x is server's secret key. Then S embeds $\{Y_i, h(\cdot)\}$ into smart card and issues the smart card to S.

Step 3. Upon receiving the smart card, U_i stores N_i and B_i into the smart card.

Login phase

When a user U_i wishes to login to the server, he inserts his smart card into the card reader and executes the login session as follows:

Step 1. U_i inputs ID_i and PW_i and imprints his biometrics B_i^* at the sensor.

Step 2. Upon receiving the inputs, the smart card verifies the condition $d(B_i, B_i^*) \geq \tau$ with the help of stored B_i, where τ is a predetermined threshold for biometrics verification. If the condition holds, it terminates the session.

Step 3. The smart card generates a random number r_i and computes $W = h(ID_i||PW_i|| B_i||N_i)$ and $X_i = Y_i \oplus h(W)$. The smart card achieves $a_i = h(ID_i||X_i||r_i)$ and sends the login message $< ID_i, a_i, r_i >$ to S.

Authentication and key agreement phase

User and server mutually authenticate each other and established a session key as follows:

Step 1. S computes $X_i = h(ID_i||x)$ and verifies $a_i \stackrel{?}{=} h(ID_i||X_i||r_i)$. If the verification does not hold, it terminates the session. Otherwise, S generates a random number r_s, computes $b_i = h(ID_i||X_i||r_i||r_s)$ and sends the message $< r_s, b_i >$ to U_i.

Step 2. Upon receiving the message $< r_s, b_i >$, the smart card verifies $b_i \stackrel{?}{=} h(ID_i||X_i||r_i||r_s)$. If the verification does not hold, the smart card stops the session. Otherwise, the smart card computes $c_i = h(ID_i||X_i||r_s||r_i)$ and the session key $sk = h(r_i||r_s||ID_i||X_i)$ then sends the message $< c_i >$ to S.

Step 3. Upon receiving the message $< c_i >$, S verifies $c_i \stackrel{?}{=} h(ID_i||X_i||r_s||r_i)$. If the verification fails, S stops the session. Otherwise, S computes the session key $sk = h(r_i||r_s||ID_i||X_i)$.

Password change phase

The legal user U_i can change his password and biometric as follows:

Step 1. First, U_i inserts his smart card into the card reader, and inputs identity ID_i and password PW_i. U_i imprints his biometrics B_i.

Step 2. Upon receiving the input, the smart card verifies the condition $d(B_i, B_i^*) \geq \tau$. If condition holds, it terminates the session.

Step 3. U_i selects a new random number N_i' and password PW_i', and imprints his new biometrics B_i'.

Step 4. Upon receiving the inputs, the smart card computes $W = h(ID_i|| PW_i||B_i||N_i)$ and $W_{new} = h(ID_i||PW_i'||B_i'||N_i')$ and $Y_i' = Y_i \oplus h(W) \oplus h(W_{new})$. Finally, the values Y_i , N_i and B_i are replaced with Y_i', N_i' and B_i', respectively.

Weaknesses of Yan et al.'s scheme

In this section, we show that Yan et al.'s scheme [17] does not satisfy the key security attribute such as efficient login phase, efficient password change phase and user anonymity. Moreover, their scheme is vulnerable to off-line password guessing attack, which is based on the following assumptions:

- An adversary is able to extract the information from the smart card [22–25].
- An adversary is able to eavesdrop all the messages between user and server transmitted via public channel. Moreover, adversary is able to modify, delete and resend all the messages, and can also reroute any message to any other entity [26].
- An adversary may be a legitimate user or an outsider [26, 27].

Due to above mentioned assumptions, an adversary can achieve the parameters from the smart card $\{Y_i, N_i, B_i, h(\cdot)\}$, and can intercept and record the messages $< ID_i, a_i, r_i >$ transmitted via public channel. With the help of these assumptions, an adversary can perform the following attacks successfully:

User anonymity

The leakage of the user's specific information enables the adversary to track the user current location and login history [28]. Although user's anonymity ensures user's privacy by preventing an attacker from acquiring user's sensitive personal information. Moreover, anonymity makes remote user authentication mechanism more robust as an attacker could not track which user is interacting with the server [29, 30].

The straightforward way to preserve anonymity is to conceal entity's real identity during communication. However, in Yan et al.'s scheme, user real identity is associated with the login message, which reveals sender information to eavesdropper. This shows that Yan et al.'s scheme does not protect user anonymity.

Off-line password guessing attack

An adversary can guess a legitimate user password with the help of achieved values $\{Y_i, N_i, B_i, h(\cdot)\}$ from the smart card and $< ID_i, a_i, r_i >$ from the intercepted message. An adversary can guess the password as follows:

Step 1. The attacker guesses the value PW_i^* and computes $X_i^* = Y_i \oplus h(h(ID_i||PW_i^*||B_i||N_i))$ then verifies $a_i \stackrel{?}{=} h(ID_i||X_i^*||r_i)$.

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

Inefficient login phase

In Yan et al.'s scheme, a smart card does not verify the correctness of input in login phase. However, a user may enter wrong password or identity due to mistake.

Case 1 If a user inputs wrong password PW_i^* due to mistake.

Step 1. U_i inputs ID_i and PW_i^* and imprints his biometrics B_i^* at the sensor.

Step 2. Upon receiving the inputs, the smart card verifies the condition $d(B_i, B_i^*) \geq \tau$ with the help of stored B_i. When biometrics verification holds, the smart card generates a random number r_i and computes $W^* = h(ID_i||PW_i^*||B_i||N_i)$ and $X_i^* = Y_i \oplus h(W^*) = X_i \oplus h(W) \oplus h(W^*) \neq X_i$ as $W \neq W^*$. The smart card also computes $a_i^* = h(ID_i||X_i^*||r_i)$. Then the smart card sends the login message $< ID_i, a_i^*, r_i >$ to S.

Step 3. S computes $X_i = h(ID_i||x)$ and verifies $a_i^* = h(ID_i||X_i||r_i)$. The verification does not hold as $X_i^* \neq X_i$. S terminates the session as authentication does not hold.

Case 2 If a user inputs the wrong identity ID_i^*, the smart card does not verify the correctness of identity and executes the session.

Step 1. U_i inputs ID_i^* and PW_i and imprints his biometrics B_i^* at the sensor.

Step 2. Upon receiving the inputs, the smart card verifies the condition $d(B_i, B_i^*) \geq \tau$ with the help of stored B_i. When biometrics verification holds, the smart card generates a random number r_i and computes $W^* = h(ID_i^*||PW_i||B_i||N_i)$ and $X_i^* = Y_i \oplus h(W^*) = X_i \oplus h(W) \oplus h(W^*) \neq X_i$ as $W \neq W^*$. Then smart card achieves $a_i^* = h(ID_i^*||X_i^*||r_i)$. Then the smart card sends the login message $< ID_i^*, a_i^*, r_i >$ to S.

Step 3. S computes $X_i' = h(ID_i^*||x)$ and verifies $a_i^* = h(ID_i^*||X_i'||r_i)$. The verification does not hold as $X_i^* \neq X_i'$. S terminates the session as authenticated does not hold.

Inefficient password and biometrics update phase

In Yan et al.'s scheme, a smart card does not verify the correctness of identity and password, and executes the password change after the successful verification of user's biometrics. However, a user may enter wrong password as human may sometimes forget the password, commit some mistake or use one account password into another account. This will cause the denial of service. Let a user inputs the wrong password PW_i^* or wrong identity ID_i^* then the following cases are possible:

i) When user U_i inputs correct identity ID_i and incorrect password PW_i^*, and imprints his biometrics B_i. The smart card only verifies the condition $d(B_i, B_i^*) \geq \tau$. When biometrics verification holds, it executes the password change phase without verifying the correctness of password as follows:

   – U_i inputs a new random number N_i', new password PW_i', and imprints his new biometrics B_i'.
   – The smart card computes $W^* = h(ID_i||PW_i^*||B_i||N_i)$, $W_{new} = h(ID_i||PW_i'||B_i'||N_i')$ and $Y_i^* = Y_i \oplus h(W^*) \oplus h(W_{new}) = X_i \oplus h(W) \oplus h(W^*) \oplus h(W_{new}) \neq X_i \oplus h(W_{new})$ as $W^* \neq W$.
   – Finally, it replaces Y_i with Y_i^*, N_i with N_i' and B_i with B_i'.

ii) When user U_i inputs incorrect identity ID_i^* and correct password PW_i, and imprints his biometrics

B_i. The smart card only verifies the condition $d(B_i, B_i^*) \geq \tau$. When biometrics verification holds, it executes the password change phase without verifying the correctness of identity as follows:

- U_i inputs a new random number N_i' and new password PW_i', and imprints his new biometrics B_i'.
- The smart card computes $W^* = h(ID_i^*|| PW_i||B_i||N_i)$, $W_{new} = h(ID_i^*||PW_i' ||B_i'||N_i')$ and $Y_i^* = Y_i \oplus h(W^*) \oplus h(W_{new})$ $= X_i \oplus h(W) \oplus h(W^*) \oplus h(W_{new}) \neq X_i \oplus h(W_{new})$ as $W^* \neq W$.
- Finally, the smart card replaces Y_i with Y_i^*, N_i with N_i' and B_i with B_i'.

iii) When user U_i inputs incorrect identity ID_i^* and incorrect password PW_i^*. If biometrics verification holds, it changes the password as follows:

- U_i inputs a new random number N_i' and new password PW_i', and imprints his new biometrics B_i'.
- The smart card computes $W^* = h(ID_i^*|| PW_i^*||B_i||N_i)$, $W_{new} = h(ID_i^*||PW_i' ||B_i'||N_i')$ and $Y_i^* = Y_i \oplus h(W^*) \oplus h(W_{new})$ $= X_i \oplus h(W) \oplus h(W^*) \oplus h(W_{new}) \neq X_i \oplus h(W_{new})$ as $W^* \neq W$.
- Finally, the smart card replaces Y_i with Y_i^*, N_i with N_i' and B_i with B_i'.

It is clear from the above discussion that in all the cases Y_i is incorrectly updated, i.e., in all the above cases $Y_i^* \neq X_i \oplus h(W_{new})$. This causes denial of service, which is clear from the following discussion:

- User inputs updated password PW_i' and identity ID_i, and also imprints his biometrics B_i'. The smart card only verifies the biometrics. When biometrics verification holds, the smart card generates a random number r_i and computes $W_{new} = h(ID_i||PW_i'||B_i'||N_i')$.
- Smart card computes $X_i^* = Y_i^* \oplus h(W_{new}) \neq X_i$ as $Y_i^* \neq X_i \oplus h(W_{new})$. Smart card also computes $a_i^* = h(ID_i||X_i^*||r_i)$ then sends the message $< ID_i, a_i^*, r_i >$ to S.
- Upon receiving the message $< ID_i, a_i^*, r_i >$, S computes $X_i = h(ID_i||x)$ and verifies $a_i^* \stackrel{?}{=} h(ID_i||X_i||r_i)$. The verification does not hold as $X_i^* \neq X_i$. Then S terminates the session.

It is clear from the above discussion that user cannot establish an authorize session with the help of the wrongly changed parameters.

Three factor authentication

The biometric based authentication schemes are designed to achieve three-factor authentication where biometric information is needed along with the password to generate a valid login message. However, in Yan et al.s scheme, only by knowing user's password, an adversary can generate a valid login message. The adversary can establish authorized session with the help of leaked password with the server as follows:

- The adversary intercepts and login message $< ID_i, a_i, r_i >$ and achieve user's identity ID_i.
- The adversary retrieves the parameters Y_i, N_i and B_i from the stolen smart card.
- The adversary computes $W = h(ID_i||PW_i||B_i||N_i)$ and retrieves the user's long-term key $X_i = Y_i \oplus h(W)$ using leaked password.
- The adversary generates a random number r_E and computes $a_E = h(ID_i||X_i||r_E)$ then sends the login message $< ID_i, a_E, r_E >$ to S.
- S computes $X_i = h(ID_i||x)$ and verifies $a_E \stackrel{?}{=} h(ID_i||X_i||r_E)$. The verification holds as $a_E = h(ID_i||X_i||r_E)$. S generates a random number r_s, computes $b_i = h(ID_i||X_i||r_E||r_s)$ and sends the message $< r_s, b_i >$ to the smart card.
- The adversary intercepts the message $< r_s, b_i >$ and computes $c_E = h(ID_i||X_i||r_s||r_E)$. He sends the message $< c_i >$ to S.
- Upon receiving the message $< c_E >$, S verifies $c_E \stackrel{?}{=} h(ID_i||X_i||r_s||r_E)$. The verification holds as $c_E = h(ID_i||X_i||r_s||r_E)$.

In general, biometric based authentication schemes support three-factor authentication where leakage of password does not enable an adversary to successfully login to the system. However by knowing user's password, an adversary can successfully login to the server in Yan et al.'s scheme. This shows that the use of unique biometric information does not enhance the security of the scheme. In other words, Yan et al.'s scheme does not achieve three-factor authentication.

Proposed scheme

In this section, we present a modified scheme to overcome the weaknesses of Yan et al.'s scheme. The proposed scheme adopts three factor security. It has similar phases like Yan et al.'s scheme. In the proposed scheme, a user first registers himself and achieves the smart card. With the help of smart card he can login to the system and establish the session. The proposed scheme executes in following four phases:

(i) Registration
(ii) Login
(iii) Authenticated key agreement
(iv) Password and biometrics update

Registration phase

A new user U_i submits his registration request to the server S. S registers the user and issues a personalized smart card to U_i as follows:

Step 1. U_i selects an identity ID_i and password PW_i of his choice, and imprint his biometrics B_i. He/She generates a random number N_i, and computes $W = h(ID_i||PW_i||N_i)$. U_i submits the registration request with ID_i and W to S via secure channel.

Step 2. S computes $X_i = h(ID_i||x)$, $Y_i = X_i \oplus W$, where x is the server's 1024-bits or 2048-bits secret key. S generates a random number R and computes user's dynamic identity by encrypting the user identity using symmetric key encryption algorithm such as AES-256, i.e., $NID = \text{Sym.Enc}_{(x)}(ID_i||R)$. The server selects the long key to resist server's secret key guessing attack. Then S embeds $\{NID, Y_i, h(\cdot)\}$ into the smart card and issues the smart card to U_i.

Step 3. Upon receiving the smart card, U_i stores $N = N_i \oplus H(B_i)$ and $V_i = h(ID_i||PW_i||N_i)$ into the smart card (Fig. 1).

Login phase

When a user U_i wishes to login to the server, he inserts his smart card into the card reader then login session executes as follows:

Step 1. U_i inputs ID_i and PW_i, and imprints his biometrics B_i at the sensor.

Step 2. The smart card computes $N_i = N \oplus H(B_i)$, and verifies $V_i \stackrel{?}{=} h(ID_i||PW_i||N_i)$. If the verification does not hold, the smart card terminates the session.

Step 3. The smart card computes $W = h(ID_i||PW_i||N_i)$ to get $X_i = Y_i \oplus W$. The smart card generates a random number r_i and computes $a_i = h(ID_i||X_i||r_i)$. Then the smart card sends the login message $< NID, a_i, r_i >$ to S (Fig. 2).

Authenticated key agreement phase

User U_i and server S performs the following steps to mutually authenticate each other:

Step 1. S retrieves ID_i by decrypting NID and computes $X_i = h(ID_i||x)$. S verifies $a_i \stackrel{?}{=} h(ID_i||X_i||r_i)$. If the verification does not hold, S terminates the session.

Step 2. S generates random numbers r_s and R', and computes $sk = h(ID_i||X_i||r_i||r_s)$, $NID' = \text{Sym.Enc}_{(x)}(ID_i||R')$ and $b_i = h(ID_i||NID||sk||NID')$. S sends the message $< r_s, b_i, h(sk||ID_i) \oplus NID' >$ to the user.

Step 3. Upon receiving the message $< r_s, b_i, h(sk||IDi) \oplus NID' >$, the smart card computes the session key $sk = h(ID_i||X_i||r_i||r_s)$ and retrieves $NID' = h(sk||ID_i) \oplus NID' \oplus h(sk||ID_i)$. Then it verifies $b_i \stackrel{?}{=} h(ID_i||NID||sk||NID')$. If the verification does not hold, the smart card stops the session. Otherwise, S is authenticated and session key sk is verified.

Step 4. The smart card computes $c_i = h(ID_i||NID'||sk)$ and sends the session key verification message $< c_i >$ to S.

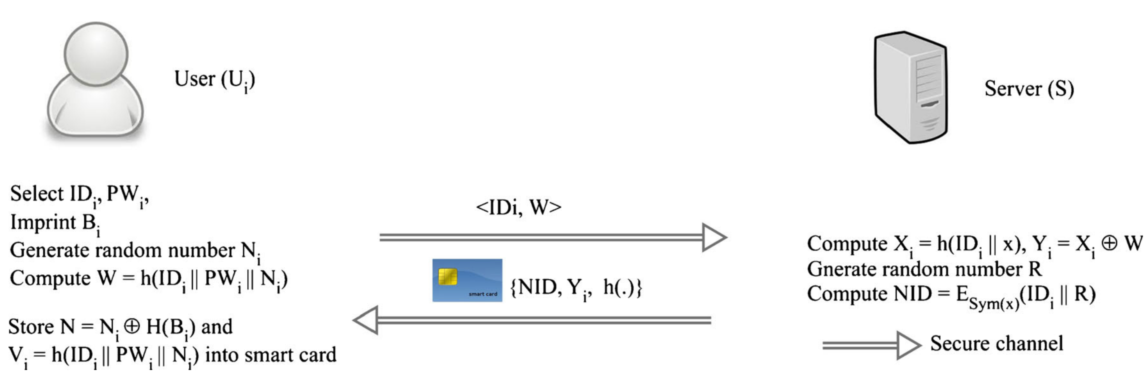

Fig. 1 The pictorial representation of registration phase

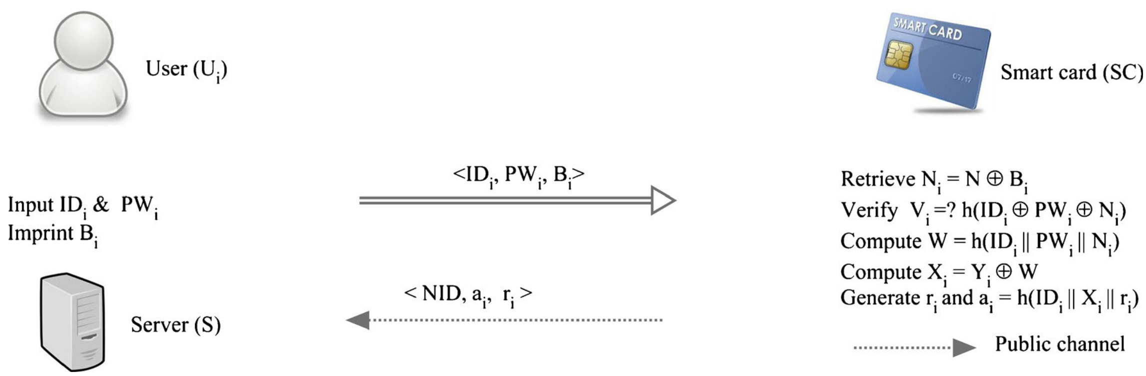

Fig. 2 The pictorial representation of login phase

Step 5. Upon receiving the message $< c_i >$, S verifies $c_i \stackrel{?}{=} h(ID_i||NID'||sk)$. If the verification fails, S stops the session. Otherwise, the session key sk is verified and U_i is authenticated (Fig. 3).

Password and biometrics update phase

The legal user can change his password and biometrics without server assistance as follows:

Step 1. U_i inserts his smart card into the card reader and inputs identity ID_i and password PW_i, and imprints his biometrics B_i.

Step 2. The smart card retrieves $N_i = N \oplus H(B_i)$ and verifies $V_i \stackrel{?}{=} h(ID_i||PW_i||N_i)$. If the verification does not hold, it terminates the session. Otherwise, it asks new parameters.

Step 3. U_i selects a new random number N_i' and password PW_i', and imprints his new biometrics B_i'.

Step 4. Upon receiving the input, the smart card computes $W = h(ID_i||PW_i||N_i)$, $W_{new} = h(ID_i||PW_i'||N_i')$, $Y_{new} = Y_i \oplus W \oplus W_{new}$, $V_{new} = h(ID_i||PW_i'||N_i')$ and $N_{new} = N_i' \oplus H(B_i')$. Finally, the smart card replaces Y_i with Y_{new}, N with N_{new} and V_i with V_{new} (Fig. 4).

Analysis

In this section, we will analyze the strength of the proposed scheme against most common attacks:

Stolen smart card attack Let the smart card of a user is stolen by an attacker. Then the attacker can extract the parameters $\{NID, Y_i, N, B, V_i, h(\cdot)\}$ from the smart card. Moreover, an attacker can intercept the login message $< NID, a_i, r_i >$. However, he can not use the stolen smart card to establish authorize session with the server using stolen smart card. This is clear from the following facts:

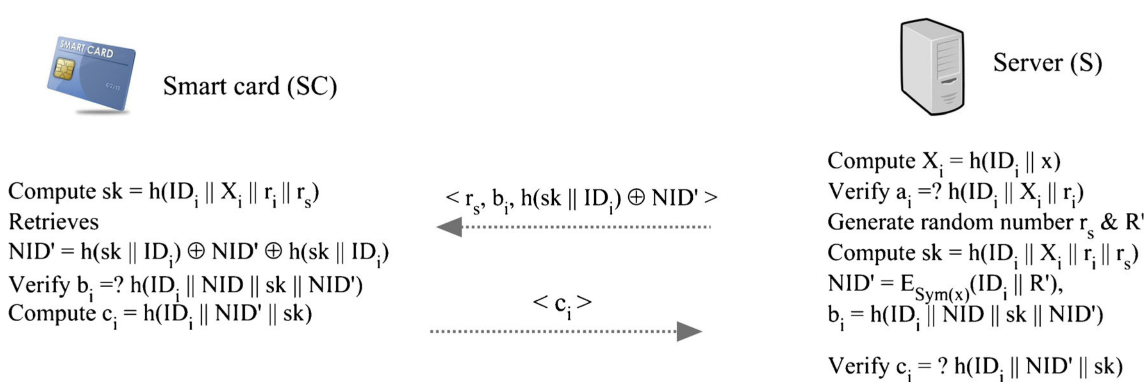

Fig. 3 The pictorial representation of authentication phase

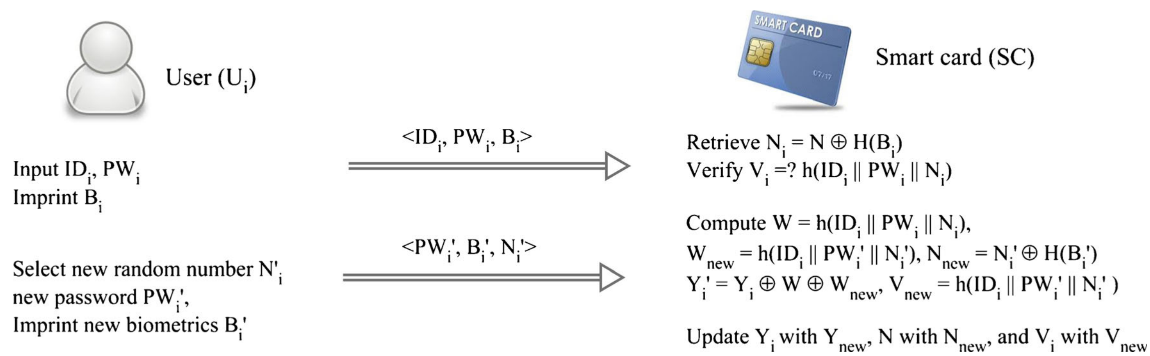

Fig. 4 The pictorial representation of password change phase

- To generate a valid login message $< NID, a_i, r_i >$, an attacker has to compute $a_i = h(ID_i||X_i||r_i)$ for a random value r_i.
- To compute a_i, the user secret key X_i is needed.
- To retrieve secret key X_i from $Y_i = X_i \oplus W$, the user password along with biometric are needed as $W = h(ID_i||PW_i||N_i)$ and $N_i = N \oplus H(B_i)$.

Since the password is only known to the user, an attacker cannot generate a valid login message using stolen smart card. This shows that the proposed scheme withstands stolen smart card attack.

On-line password guessing attack An active adversary may try to guess a user's password using on-line password guessing attack with the achieved information $\{NID, Y_i, N, B, V_i, h(\cdot)$ and $\{NID, a_i, r_i\}$. However, the on-line password guessing attack will not succeed in the proposed scheme. This is justified from the following discussion:

- Let the adversary E guesses the user's password PW^*.
- To verify the user's guessed password PW^*, E has to generate a valid login message $< NID, a_i, r_i >$, where $a_i = h(ID_i||X_i||r_i)$. This is equivalent to achieve X_i and ID_i using the values $NID = E_{\mathsf{Sym(x)}}(ID_i||R)$, N and Y_i.
- NID is encrypted with server key where server secret key is unknown to the attacker. Therefore, an attacker cannot achieve ID_i and so N_i and B_i.
- To achieve X_i from $Y_i = X_i \oplus W$, An attacker has to compute W^* using guessed password PW^*. Computation of W^* requires ID_i and B_i as $W^* = h(ID_i||PW_i^*||N_i)$ and $N_i = N \oplus H(B_i)$. Thus an attacker cannot achieve X_i with the help of guessed password as ID_i and B_i are secret.

It is clear that an attacker cannot achieve required parameters for on-line password guessing attack. This shows that the proposed scheme resist on-line password guessing attack.

Off-line password guessing attack A passive adversary may try to guess a user's password in off-line mode. However, he cannot verify the guessed password correctly using achieved parameters $\{NID, Y_i, N, B, V_i, h(\cdot)$ and $\{NID, a_i, r_i\}$. This is clear from the following facts:

- Let the attacker E guesses the user's password as PW^*.
- To verify this guessed password PW^* with the condition $V_i = h(ID_i||PW_i||N_i)$ is equivalent to achieve ID_i from NID and N_i from N.
- The server secret key x is requires to achieve ID_i from NID as $NID = \text{Sym.Enc}_{(x)}(ID_i||R)$. Moreover, to achieve N_i from N, B_i is required as $N = N_i \oplus H(B_i)$.

It is clear from the discussion that an adversary cannot guess user's password correctly as user's identity and biometric are not with attacker.

Replay attack An adversary can eavesdrop user's communication can intercept and record old communications $< NID, a_i, r_i >$, $< r_s, b_i >$ and $< c_i >$. Then he can try to replay the message. However, this attempt will not succeed due to the following facts:

- Let adversary replay the message $< NID, a_i, r_i >$ and sends to S.
- Upon receiving the message $< NID, a_i, r_i >$, S achieves $ID_i||R = \text{Sym.Dec}_{(x)}(NID)$, retrieve ID_i and computes $X_i = h(ID_i||x)$. S verifies $a_i \stackrel{?}{=} h(ID_i||X_i||r_i)$. The verification holds as an adversary replays the user's login message without any change.
- S generates a random number r_s' and computes $sk' = h(ID_i||X_i||r_i||r_s')$, $NID' = \text{Sym.Enc}_{(x)}(ID_i||R')$ and $b_i' = h(ID_i||NID||sk'||NID')$ and sends the message $< r_s', b_i', h(sk||ID_i) \oplus NID' >$ to the user.
- Adversary intercepts the message $< r_s', b_i', h(sk||ID_i) \oplus NID' >$ and try to respond by sending the message $< c_i' >$, where

$c_i' = h(ID_i||NID'||sk')$. However, an adversary cannot compute $< c_i' >$ from the known parameters $\{NID, Y_i, N, B, V_i, h(\cdot), \{NID, a_i, r_i\}$ and $< r_s', b_i', h(sk||ID_i) \oplus NID' >$, which is clear from the following discussion:

- To compute $c_i' = h(ID_i||NID'||sk')$ is equivalent to compute $sk' = h(ID_i||X_i||r_i\ ||r_s')$.
- To compute $sk' = h(ID_i||X_i||r_i||r_s')$, user identity ID_i and user's secret key X_i are needed. The user identity ID_i is encrypted with server's secret key and user's secret key is protected with the password and biometrics, *i.e.*, $X_i \oplus h(ID_i||PW_i||N_i)$, where $N_i = N \oplus H(B_i)$.
- User biometrics B_i and password PW_i are secret, therefore an adversary cannot compute $< c_i' >$.

- Since the adversary cannot respond with the valid message $< c_i' >$, the server terminates the session.

Mutual authentication In mutual authentication mechanism, the user must prove its identity to the server and the server must prove its identity to the user. In the proposed scheme, user and server both authenticate each other using the following conditions:

$$b_i \stackrel{?}{=} h(ID_i||NID||sk||NID')$$
$$c_i \stackrel{?}{=} h(ID_i||NID'||sk)$$

To forge an user or server an adversary has to compute b_i or c_i, respectively. However, to compute b_i or c_i, an adversary has to compute $sk = h(ID_i||X_i||r_i||r_s)$ which requires the information of user's secret key X_i. Since user's secret key X_i is protected, only authorized principals can compute b_i and c_i. This shows that user and server can correctly verify the authenticity of each other.

Efficient login phase In the proposed scheme, smart cards can easily identify the incorrect input as follows:

Case 1 If the smart card receives wrong biometrics B_i^*, the session is terminated as follows:

- The smart card retrieves $N_i^* = N \oplus H(B_i^*)$.
- The smart card verifies $V_i \stackrel{?}{=} h(ID_i||PW_i||N_i^*)$. The condition does not hold as $V_i = h(ID_i||PW_i||N_i)$ and $N_i \neq N_i^*$ and the smart card terminates the session.

Case 2 If the smart card receives incorrect password PW_i^*, the session is terminated as follows:

- The smart card achieves $N_i = N \oplus H(B_i)$ and verifies $V_i \stackrel{?}{=} h(ID_i||PW_i^*||N_i)$.
- The verification does not hold as $V_i = h(ID_i||PW_i||N_i)$ and $PW_i^* \neq PW_i$.

Case 3 If the smart card receives incorrect identity ID_i^*, the session is terminated as follows:

- The smart card retrieves $N_i = N \oplus B_i$ and verifies $V_i \stackrel{?}{=} h(ID_i^*||PW_i||N_i)$.
- The verification does not hold as $V_i = h(ID_i||PW_i||N_i)$ and $ID_i^* \neq ID_i$.

In all the above cases the smart card can detect the incorrect input. This shows that proposed scheme has efficient login phase.

User-friendly and efficient password and biometrics changes phase In the proposed scheme, the user is allowed to change his password without server assistance. This makes proposed scheme user-friendly. Moreover, the smart card verifies the correctness of identity, password and biometrics before changing the password. Since the smart card can verify the correctness of input efficiently, a user can change his password and biometrics correctly without any mistake.

Session key agreement & verification Both the user and server compute the session key $sk = h(ID_i||X_i||r_i||r_s)$ and verifies it using the following conditions

$$b_i = h(ID_i||NID||sk||NID')$$
$$c_i = h(ID_i||NID'||sk)$$

To compute b_i or c_i, an adversary has to compute $sk = h(ID_i||X_i||r_i||r_s)$. To compute $sk = h(ID_i||X_i||r_i||r_s)$, user's secret key X_i is needed. Since user's secret key is protected, only authorized principals can compute b_i and c_i. This shows that user and server can correctly verify the established session key.

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 a_i. To compute a_i, user's secret key X_i is needed. To achieve X_i from Y_i, the correct password PW_i along with fingerprint B_i and identity ID_i are needed. Thus the compromised password does not enable an adversary to compute a valid login message, which is clear from the following points:

- Let an adversary achieves user's password PW_i and the smart card.
- Let the adversary extracts the secrets $\{NID, Y_i, N, B, V_i\}$ from the smart card.

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

Security attributes\Schemes	[31]	[32]	[33]	[34]	[16]	[17]	Proposed scheme
User anonymity	×	×	√	√	×	×	√
Insider Attack	×	√	√	×	√	√	√
Stolen smart card attack	√	√	√	√	√	√	√
Replay attack	√	√	√	√	√	√	√
Off-line password guessing attack	√	√	√	×	√	×	√
Mutual authentication	×	√	√	√	√	√	√
User-friendly password selection	√	√	√	√	√	√	√
Session key agreement	×	√	√	×	√	√	√
Session key verification	–	×	×	×	×	×	√
Efficient login phase	×	×	×	×	×	×	√
Efficient password change phase	×	×	×	×	×	×	√
Biometric update phase	–	–	–	–	√	√	√
Three factor authentication	×	×	√	×	√	×	√

- The adversary generates a random number r_E and may try to generate the login message $< NID, a_i', r_E >$ with the help of compromised password PW_i. However, to compute $a_i = h(ID_i||X_i||r_E)$, user secret key X_i along with identity is needed. To retrieve X_i from $Y_i = X_i \oplus W$, adversary has to compute W . Computation of W requires identity ID_i and biometric B_i as $W = h(ID_i||PW_i||N_i)$ and $N_i = N \oplus H(B_i)$.
- The adversary cannot achieve N_i form $N = N_i \oplus H(B_i)$ due to uniqueness property of biometric keys.

This shows that to generate a valid login message, both the security parameters, password and biometric are needed along with stolen smart card. This shows that the proposed scheme achieves three-factor authentication.

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 password PW_i and biometrics B_i in its original form, i.e., user submits $W = h(ID_i||PW_i||N_i)$ instead of PW_i and B_i to the registration authority. Thus an insider can neither guess the password PW_i nor retrieve it from W as hash function is one way and N_i is unknown. This shows that the proposed scheme resists insider attack.

User anonymity The login message $< NID, a_i, r_i >$ includes user's dynamic identity $NID = \text{Sym.Enc}_{(x)}(ID_i||R)$ instead of original identity ID_i. To achieve ID_i from NID server's secret key x is needed as ID_i is encrypted using the key x. Since the server's secret

Table 3 Security attributes comparison with some password based authentication schemes for TMIS

Security attributes\Schemes	[8]	[11]	[35]	[5]	[4]	[10]	[7]	Proposed scheme
User anonymity	×	×	√	√	√	√	√	√
Insider Attack	√	√	√	√	√	√	√	√
Off-line password guessing attack	×	√	√	√	×	×	√	√
Stolen smart card attack	√	√	√	√	√	√	√	√
Replay attack	√	√	√	√	×	√	√	√
Mutual authentication	√	√	√	√	√	√	√	√
Session key agreement	√	×	√	√	√	√	√	√
Session key verification	√	–	√	×	√	×	×	√
Efficient login	×	×	×	√	×	×	×	√
Efficient password change	×	×	×	√	√	×	×	√
User-friendly password change	×	×	×	√	×	√	√	√

Table 4 Computation cost comparison of the proposed scheme with some biometric based authentication schemes

Phases\ Schemes	[31]	[32]	[33]	[34]	[16]	[17]	Proposed scheme
Registration	$3T_h$	$4T_h$	$5T_h$	$T_H + 3T_h$	$4T_h$	$3T_h$	$3T_h + T_H + T_S$
Login	$2T_h$	$4T_h$	$5T_h$	$T_H + 2T_h$	$3T_h + T_S$	$3T_h$	$3T_h + T_H$
Authentication	$5T_h$	$7T_h$	$9T_h$	$7T_h$	$8T_h + T_S$	$8T_h$	$10T_h + 2T_S$
Password Change	$3T_h$	$4T_h$	$4T_h$	$T_H + 2T_h$	$6T_h$	$4T_h$	$4T_h + 2T_H$

key x is secret, nobody other than the server can achieve user's identity from the login message. This dynamic identity concept protect anonymity.

Comparison

If the scheme prevents attack or satisfies the property, the symbol '$\surd$' is used and if it fails to prevent attack or does not satisfy the attribute, the symbol $\times$ is used.

We will compare the security attributes of our scheme with some biometric based authentication schemes such as Li and Hwang's [31], Li et al.'s [32], Troung et al.'s [33], Chang's et al.'s [34] and Yan et al.'s [17] schemes in Table 2.

We compare our scheme with some recently published password based schemes for TMIS [4, 5, 7, 8, 10, 11, 35] in Table 3.

We show the efficiency analysis of proposed schemes with some relevant schemes in Table 4, 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 [36, 37]. Since the computation overhead of XOR is relatively very less, so we are ignoring the computation of XOR operation in our comparison.

Conclusion

In this paper, we have analyzed Yan et al.'s scheme and demonstrated that the weaknesses of their scheme. Further, we have presented an improvement of Yan et al.'s scheme for TMIS to eliminate the drawbacks of their scheme. The proposed scheme efficiently identifies the correctness of input and present efficient login and password change phase. Moreover, the proposed scheme protects anonymity and resists password guessing attack where Yan et al.'s scheme failed.

Acknowledgments The authors thank the anonymous referees for their valuable comments that helped to improve the presentation of the paper. Third author (Dr. Ankita Chaturvedi) is thankful to National Board for Higher Mathematics (NBHM), Mumbai, India, for their financial support. One co-author (Dr. Muhammad Khurram Khan) research was partially funded by National Natural Science Foundation of China (NSFC) under Grant no. 61300220 and 61371098.

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

References

1. Leng, L., Teoh, A.B.J., Li, M., Khan, and M.K., A remote cancelable palmprint authentication protocol based on multi-directional two-dimensional palmphasor-fusion. *Sec. Commun. Netw.*, 2013. doi:10.1002/sec.900
2. Khan, M.K., and Kumari, S., An authentication scheme for secure access to healthcare services. *J. Med. Syst.* 37(4):1–12, 2012
3. Kumari, S., Khan, M.K., and Kumar, R., Cryptanalysis and improvement of a privacy enhanced scheme for telecare medical information systems. *J. Med. Syst.* 37(4):1–11,2012
4. Cao, T., and 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., and 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. Debiao, H., Jianhua, C., and Rui, Z., A more secure authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(3):1989–1995, 2012
7. Lin, H.Y., On the security of a dynamic ID-based authentication scheme for telecare medical information systems. *J. Med. Syst.* 37(2):1–5, 2013
8. Wei, J., Hu, X., and Liu, W., An improved authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(6):3597–3604, 2012
9. Wu, Z.Y., Lee, Y.C., Lai, F., Lee, H.C., and Chung, Y., A secure authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(3):1529–1535, 2012
10. Xie, Q., Zhang, J., and Dong, N., Robust anonymous authentication scheme for telecare medical information systems. *J. Med. Syst*. 37(2):1–8, 2013
11. Zhu, Z., An efficient authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(6):3833–3838, 2012
12. Leng, L., Zhang, J., Khan, M.K., Chen, X., Ji, M., and Alghathbar, K., Cancelable palmcode generated from randomized gabor filters for palmprint template protection. *Sci. Res. Ess.* 6(4):784–792. 2011
13. Leng, L., and Zhang, J., Palmhash code vs. palmphasor code. *Neurocomput.*, 2012

14. Khan, M.K., Zhang, J., and Alghathbar, K., Challenge-response-based biometric image scrambling for secure personal identification. *Futur. Gener. Comput. Syst.* 27(4):411–418, 2011
15. Khan, M.K., Zhang, J., and Tian, L., Protecting biometric data for personal identification. In: *Advances in Biometric Person Authentication*: Springer, 629–638, 2005
16. Tan, Z., An efficient biometrics-based authentication scheme for telecare medicine information systems. *Network* 2(3):200–204,2013
17. Yan, X., Li, W., Li, P., Wang, J., Hao, X., and Gong, P., A secure biometrics-based authentication scheme for telecare medicine information systems. *J. Med. Syst.* 37(5):1–6, 2013
18. Jin, A.T.B., Ling, D.N.C., and Goh, A., Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recog.* 37(11):2245–2255, 2004
19. Belguechi, R., Rosenberger, C., and Ait-Aoudia, S., Biohashing for securing minutiae template. In: *20th International Conference on Pattern Recognition (ICPR)*, 1168–1171, 2010
20. Lumini, A., and Nanni, L., An improved biohashing for human authentication. *Pattern Recogn.* 40(3):1057–1065, 2007
21. Yang, C., *Integration of Biometrics and Pin Pad on Smart Card*. PhD thesis: University of Newcastle Upon Tyne, 2011
22. Brier, E., Clavier, C., and Olivier, F., Correlation power analysis with a leakage model. In: *Cryptographic Hardware and Embedded Systems-CHES*: Springer, 16–29, 2004
23. Eisenbarth, T., Kasper, T., Moradi, A., Paar, C., Salmasizadeh, M., and 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*: Springer, 203–220, 2008
24. Kocher, P., Jaffe, J., and Jun, B., Differential power analysis. In: *Advances in CryptologyCRYPTO99*: Springer, 388–397, 1999
25. Messerges, T.S., Dabbish, E.A., and Sloan, R.H., Examining smart-card security under the threat of power analysis attacks. *IEEE Trans. Comput.* 51(5):541–552, 2002
26. Boyd, C., and Mathuria, A., *Protocols for Authentication and Key Establishment*: Springer, 2003
27. Yang, C.C., Yang, H.W., and Wang, R.C., Cryptanalysis of security enhancement for the timestamp-based password authentication scheme using smart cards. *IEEE Trans. Consum. Electron.* 50(2):578–579, 2004
28. Juang, W.S., Lei, C.L., and Chang, C.Y., Anonymous channel and authentication in wireless communications. *Comput. Commun.* 22(15):1502–1511, 1999
29. Khan, M.K., Kim, S.K., and Alghathbar, K., Cryptanalysis and security enhancement of a ‘more efficient & secure dynamic ID-based remote user authentication scheme. *Comput. Commun.* 34(3):305–309, 2011
30. Xu, J., Zhu, W.T., and Feng, D.G., An efficient mutual authentication and key agreement protocol preserving user anonymity in mobile networks. *Comput. Commun.* 34(3):319–325, 2011
31. 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
32. Li, X., Niu, J.W., Ma, J., Wang, W.D., and 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
33. Truong, T.T., Tran, M.T., and Duong, A.D., Robust biometrics-based remote user authentication scheme using smart cards. In: *15th International Conference on Network-Based Information Systems (NBiS)*, 384–391, 2012
34. Chang, Y.F., Yu, S.H., and Shiao, D.R., A uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care. *J. Med. Syst.* 37(2):1–9, 2013
35. Lee, C.C., and Hsu, C.W., A secure biometric-based remote user authentication with key agreement scheme using extended chaotic maps. *Nonlinear Dyn.* 71(1–2):201–211, 2013
36. Potlapally, N.R., Ravi, S., Raghunathan, A., and Jha, N.K., A study of the energy consumption characteristics of cryptographic algorithms and security protocols. *IEEE Trans. Mobile Comput.* 5(2):128–143, 2006
37. Wong, D.S., Fuentes, H.H., and Chan, A.H., The performance measurement of cryptographic primitives on palm devices. In: *17th Annual Computer Security Applications Conference (ACSAC-2001)*, 92–101, 2001