Improved Biometric-Based Three-factor Remote User Authentication Scheme with Key Agreement Using Smart Card

Ankita Chaturvedi, Dheerendra Mishra, and Sourav Mukhopadhyay

Department of Mathematics,
Indian Institute of Technology Kharagpur, Kharagpur-721302, India
ankitac17@gmail.com, {dheerendra,sourav}@maths.iitkgp.ernet.in

Abstract. Remote user authentication is a very important mechanism in the network system to verify the correctness of remote user and server over the insecure channel. In remote user authentication, server and user mutually authenticate each other and draw a session key. In 2012, An presented a biometric based remote user authentication scheme and claimed that his scheme is secure. In this article, we analyze An's scheme and show that his scheme is vulnerable to known session specific temporary information attack, forward secrecy attack. Moreover, we also identify that An's scheme fails to ensure efficient login phase and user anonymity. Recently, Li et al. also presented a biometric based three-factor remote user authentication scheme with key agreement. They claimed that their scheme provides three-factor remote user authentication. However, we analyze and find that scheme does not achieve three-factor remote user authentication and also fails to satisfy key security attributes. Further, the article presents an improved anonymous authentication scheme which eliminates all the drawbacks of An's and Li et al.'s scheme. Moreover, proposed scheme presents efficient login and password change mechanism where incorrect password input can be quickly detected and user can freely change his password.

Keywords: Network security, Smart card, Mutual authentication, Anonymity, Biometric, Password.

1 Introduction

The rapid development in network and communication technology has presented the platform for electronic commerce, e-medicine, e-education, e-learning and so forth. Most of the services adopt smart card based remote user authentication to facilitate secure services over the insecure public network. In general, smart card based authentication faces various attacks, a few are stolen smart card attack, password guessing attack and insider attack [1, 2]. These attacks are based on the following assumptions that is discussed by Xu et al. [3]: (A) An attacker can completely control the communication channel between user and server in login and verification phase, that is, it is capable of intercepting, modifying and

A. Bagchi and I. Ray (Eds.): ICISS 2013, LNCS 8303, pp. 63–77, 2013.

deleting the message. (B) An attacker may steel user's smart card and extract the stored values from it using one of the several techniques, a few are in [4, 5].

Instead of above mentioned assumptions, an efficient and secure anonymous user authentication scheme should meet the following requirements: (a) low computation and communication overhead with less storage requirement; (b) user anonymity during login and verification; (c) efficient login phase to detect incorrect login quickly; (d) resistance to different kinds of attacks; (e) user-friendly and efficient password change phase; (f) efficient mutually authenticate and session key agreement.

To provide smart card security, many password based authentication scheme have been proposed [1, 2, 6, 7, 8], which are widely employed because of their efficiency. The password based authentication schemes provide two-factor remote user authentication while biometric based user authentication schemes provide three-factor authentication [9]. Moreover, biometric uniqueness property increases its application in authentication protocols. Therefore, biometric-based remote user authentication schemes with password have attractive significant research attention. Recently, many biometric based authentication schemes have been proposed, a few are [2, 6, 7, 9, 10, 11, 12, 13, 14, 15, 16, 17]. These schemes have advantages of biometric keys (fingerprint, face, iris, hand geometry and palm-print, etc.), which are having following advantages: (i) biometric keys cannot be lost or forgotten; (ii) biometric keys can not be copied or shared easily; (iii) biometric keys are extremely difficult to forge or distribute; (iv) biometric keys maintain uniqueness property (v) biometric keys are hard to guess. These advantages suggest that biometric-based remote user authentications are more secure and reliable rather than traditional password-based remote user authentication.

In 2010, Li and Hwang presented a biometric based remote user authentication scheme [14], which uses user biometric identification to verify the correctness of valid user. In 2011, Li et al. [10] and Das [6] demonstrated the weaknesses of Li and Hwang's scheme and proposed a new efficient and secure protocols, independently. In 2012, An [12] demonstrated the weaknesses of Das's scheme and pointed out that Das's scheme does not resist password guessing, user impersonation, server masquerading and insider attack, and fails to achieve mutual authentication. In 2012, An [18] also demonstrated the security weaknesses of Lee et al.'s scheme and showed that Lee et al.'s scheme is vulnerable to offline password guessing attack, forgery attack and insider attack. An also presented an improved biometric based remote user authentication and key agreement scheme and claimed that his scheme is relatively more secure than related authentication schemes. Recently, Li et al. [9] showed that Das's scheme is vulnerable to forgery and stolen smart card attack. Additionally, they have presented an improved scheme.

2 Review of Li et al.'s Scheme

In this section, we will present a brief review of Li et al.'s scheme [9]. Li et al presented the improvement of Das's scheme [6]. In their scheme, registration

center R selects three parameters p, q and g such that q divides $p-1$ and g is a primitive element of $GF(q)$. Then, it chooses its master key X and provides the parameters p, q, g and X to the server.

2.1 Registration Phase

Step 1. U selects his identity ID_U and password PW_U. He also imprints biometric information B_U to the fuzzy extractor and achieves $Gen(B_U) = (R_U, P_U)$. Then, he computes $D_U = h(PW_U||R_U)$ and $h(R_U||N)$ and submits ID_U, P_U, $h(R_U||N)$ and D_U to S via secure channel.

Step 2. R computes $H = h(ID_U||X)$ and $e = h(ID_U||X) \oplus h(R_U||N)$. Then, R issues a smart card to U including the security parameters $\{e, P_U, D_U, h(\cdot), p, q, g\}$.

Step 3. On receiving the smart card, U stores N into the smart card.

2.2 Login Phase

Step 1. U inputs ID_U and PW_U, and imprints B_U at fuzzy extractor and calculates $R_U = Rep(B_U, P_U)$, then the smart card verifies $D_U =? h(PW_U||R_U)$. If condition holds, goto next step.

Step 2. Smart card achieves $M_1 = e \oplus h(R_U||N) = h(ID_U||X)$. Smart card generates a random number y, then computes $M_2 = g^y \bmod p \oplus M_1$ and $M_3 = h(M_1||M_2)'$. Then, U sends the login message $< ID_U, M_2, M_3 >$ to S.

2.3 Authentication and Session Key Agreement Phase

Step 1. S verifies the ID_U format. If ID_U is valid, S computes $M_4 = h(ID_U||X)$ and then verifies $M_3 =? h(h(ID_U||X)||M_2)$. If verification holds, goto next step.

Step 2. S generates a random number z and computes $M_5 = M_2 \oplus M_4$, $Z = g^z \bmod p$, $M_6 = M_5 \oplus Z$ and $M_7 = h(ID_U||ID_S||Z)$, then sends the message $< M_6, M_7 >$ to U, where ID_S is the server identity.

Step 3. Smart card achieves $M_8 = Y \oplus M_6$ and verifies $M_7 =? h(ID_U||ID_S||M_8)$. If verification holds, it computes $M_9 = h(ID_U||ID_S||h(M_8^y \bmod p))$ and sends M_9 to S.

Step 4. S verifies $M_9 =? h(ID_U||ID_S||h(M_5^z \bmod p))$. If verification holds, S accepts C's login.

Step 5. User and server computes the session key $sk_{SU} = h(M_1||ID_S||(g^z)^y \bmod p)$ and $sk_{US} = h(M_4||ID_S||(g^y)^z \bmod p)$, respectively.

2.4 Password Change Phase

- Step 1. U inputs ID_U and PW_U, and imprint B_U at fuzzy extractor and calculate $R_U = Rep(B_U, P_U)$, then the smart card verifies $D_U =? h(PW_U||R_U)$. If condition holds, goto next step.
- Step 2. U inputs a new password PW_U^{new}, then smart card computes $D_U^{new} = h(PW_U^{new}||R_U)$ and replaces D_U with D_U^{new}.

3 Cryptanalysis of Li et al.'s Scheme

In this section, we show that Li et al.'s Scheme [9] does not satisfy the key security attribute.

3.1 Three Factor Authentication

Li et al. claimed that their proposed scheme achieves three factor remote user authentication. In three factor authentication, at least three security parameters are needed to generate valid login message. In other words, user's smart card, password and biometric information are needed to generate a valid login message. However, in Li et al.'s scheme, an attacker(E) with stolen smart card and user biometric information (B_U), can generate valid login message as follows:

- E can extract the information $\{e, P_U, D_U, h(\cdot), p, q, g, N\}$ from the stolen smart card [4, 5, 19].
- E inputs B_U at fuzzy extractor and calculate $R_U = Rep(B_U, P_U)$, as P_U achieved from stolen smart card.
- E computes $h(R_U||N)$ and then $M_1' = e \oplus h(R_U||N) = h(ID_U||X)$. E also selects a random number y_E and computes $M_2' = g^{y_E} \bmod p \oplus M_1$ and $M_3' = h(M_1||M_2)$.
- E sends the login message $< ID_U, M_2', M_3' >$ to S.
- Upon receiving the message $< ID_U, M_2', M_3' >$, S verifies the ID_U format. This holds, as ID_U is extracted from user's smart card. S computes $M_4 = h(ID_U||X)$ and then verifies $M_3 =?\ h(h(ID_U||X)||M_2')$. The verification holds, as $M_1' = h(ID_U||X)$.

This above discussion concludes that without knowing the user's password, an attacker can generate valid login message. This proves that Li et al.'s scheme does not achieve three factor remote user authentication.

3.2 Known Session Specific Temporary Information Attack

The compromise of a short-term secret (session secret values) information should not compromise the generated session key [20, 21, 22, 23]. However, in Li et al.'s scheme, if short term session values (temporary secret) y or z are compromised, then an attacker can achieve the session key sk_{US} and sk_{SU}.
Case 1: If session secret (temporary information) y is compromised, then

- E can intercept and record the transmitted messages $< ID_U, M_2, M_3 >$ and $< M_6, M_7 >$, which transmits via public channel.
- E computes $g^y \bmod p$ and then achieve $h(ID_U||X) = M_2 \oplus g^y \bmod p$ and $g^z \bmod p = M_6 \oplus g^y \bmod p$.
- E computes $sk_{US} = h(h(ID_U||X)||ID_S||(g^z)^y \bmod p)$. E can also achieve sk_{SU}, as $sk_{SU} = sk_{US}$.

Case 2: If session secret z is compromised, then

- E computes $g^z \bmod p$ and then achieve $g^y \bmod p = M_6 \oplus g^z \bmod p$ and $h(ID_U||X) = M_2 \oplus g^y \bmod p$.
- E computes $sk_{SU} = h(h(ID_U||X)||ID_S||(g^y)^z \bmod p)$. E can also achieve sk_{US}, as $sk_{SU} = sk_{US}$.

3.3 Replay Attack

Replay attack is most common attack in which attacker used the past messages to forge the server [24, 25, 26].

An attacker can track, intercept, modify and record the message that transmits via public channel. Let the attacker has achieved a previously transmitted message $< ID_U, M_2', M_3' >$, where $M_2' = h(ID_U||X) \oplus Y'$ and $M_3' = h(M_1||M_2')$. Then, he replays the message $< ID_U, M_2', M_3' >$ by sending it to server. On receiving the message $< ID_U, M_2', M_3' >$, S verifies the ID_U format. The validation holds, as the message is originally generated by user. Then, S computes $M_4 = h(ID_U||X)$ and achieves $M_5' = M_2' \oplus M_4$, $Z = g^z \bmod p$, $M_6 = M_5' \oplus Z$ and $M_7 = h(ID_U||ID_S||Z)$, then sends the message $< M_6, M_7 >$ to U. The server accepts the old messages, this shows that Li et al.'s scheme does not resist replay attack.

3.4 User Anonymity

The leakage of the user's specific information, enables the adversary to track the user's current location and login history [27, 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 attacker could not track 'which users are interacting' [29, 30, 31].

The straightforward way to preserve anonymity is to conceal entities real identity during communication. However, in Li et al.'s scheme, user real identity is associated with the login message which reveals user's information to attacker. This shows that Li et al.'s scheme does not ensure user anonymity.

3.5 Inefficient Login Phase

In Li et al.'s scheme, smart card does not verify the correctness of identity in login phase. If a user inputs incorrect identity due to mistake, the smart card executes the login phase as follows:

- U inputs incorrect identity ID_U^* and PW_U, and imprints B_U at fuzzy extractor, then calculates $R_U = Rep(B_U, P_U)$. The smart card verifies $D_U = ?\ h(PW_U||R_U)$, which holds as user inputs correct identity and password.
- Smart card achieves $M_1 = e \oplus h(R_U||N) = h(ID_U||X)$. Smart card generates a random number y, then computes $M_2 = g^y \bmod p \oplus M_1$ and $M_3 = h(M_1||M_2)$. Finally, it sends the login message $< ID_U^*, M_2, M_3 >$ to S.

Instead of incorrect login input, the smart card successfully executes the login session. This causes extra communication and computation overhead.

4 Review of An's Scheme

In 2012, An [18] proposed an improvement of Lee el al.'s [10] biometric based user authentication scheme. This comprises of three phases similar to the Lee et al.'s scheme, which are as follows: registration, login, authentication. The brief description of An's scheme is as follows:

4.1 Registration Phase

Before starting the registration, the trusted registration center R generates a large prime p and selects a primitive element g of $GF(p)$.Then, a user registers with registration center as follows:

Step 1. U generates a random number N and submits ID_U, $W = h(PW_U \oplus N)$ and $f = h(B_U)$ to S.
Step 2. S computes $J = h(PW_U \oplus N)||f$ and $e = h(ID_U||X) \oplus J$, where X is server's secret key. S issues a smart card, which includes the values $\{ID_U, f, e, h(\cdot), p, g\}$ and provides the smart card to the user.
Step 3. On receiving the smart card, U stores N into the smart card.

4.2 Login Phase

Step 1. U inputs his B_U, smart card verifies $f =?h(B_U)$. If condition holds, smart card passes biometric information.
Step 2. U inputs ID_U and PW_U, then smart card computes $J = h(PW \oplus N)||f$ and achieves $M_1 = h(ID_U||X) = e \oplus J$. Smart card generates a random number r_U, then computes $M_2 = M_1 \oplus r_U$ and $M_3 = g^{r_U} \bmod p$. U sends the login message $< ID_U, M_2, M_3 >$ to S.

4.3 Authentication Phase

Step 1. S verifies the ID_U format. If ID_U is valid, S computes $M_4 = h(ID_U||X)$ and $r'_U = M_2 \oplus M_4$, then verifies $M_3 =? \ g^{r'_U} \bmod p$. If verification holds, S generates r_S and computes $M_5 = M_4 \oplus r_S$ and $M_6 = g^{r_S} \bmod p$, then sends the message $< M_5, M_6 >$ to U. S also computes session key $sk_{US} = (g^{r_U})^{r_S} \bmod p$.
Step 3. Smart card computes $r'_S = M_1 \oplus M_5$ and verifies $M_6 =? \ g^{r'_S} \bmod p$. If verification holds, it computes the session key $sk_{SU} = (g^{r_S})^{r_U} \bmod p$.

5 Cryptanalysis of An's Scheme

In this section, we show that An's Scheme [18] does not satisfy the key security attribute.

5.1 Known Session Specific Temporary Information Attack

The compromise of a short-term secret (session secret values) information should not compromise the generated session key [20, 21, 22, 23]. However, in An's scheme, if short term session values $g^{r_U} \bmod p$ or $g^{r_S} \bmod p$ are compromised, then an attacker can achieve the session key sk_{US} or sk_{SU} as follows:

- Attacker can intercept the message and record the transmitted messages $< M_2, M_3 >$ and $< M_5, M_6 >$, which transmits via public channel.
- Attacker can compute $sk_{SU} = (g^{r_S})^{r_U} \bmod p$ or $sk_{US} = (g^{r_U})^{r_S} \bmod p$ using public values and lacked values.

5.2 Forward Secrecy

The compromise of static private key of a user does not result the compromise of established session key [21, 22, 23]. Although if static private key $h(ID_U||X)$ of a user U is compromised, then An's scheme does not resist forward secrecy and an attacker can achieve the session key with the help of static private key as follows:

- Attacker can intercept the message and record the transmitted messages $< M_2, M_3 >$ and $< M_5, M_6 >$, which transmits via public channel.
- Attacker can achieve r_U and r_S as:
  $r_U = M_2 \oplus h(ID_U||X) = M_1 \oplus r_U \oplus h(ID_U||X)$,
  $r_S = M_5 \oplus h(ID_U||X) = M_4 \oplus r_S \oplus h(ID_U||X)$, as $M_1 = M_4 = h(ID_U||X)$.
- Attacker can compute $sk = g^{r_S r_U} \bmod p$, using r_U and r_S.

5.3 Replay Attack

An attacker can track, intercept, modify and record the message that transmits via public channel. Let the attacker achieved a previously transmitted message $< ID_U, M_2', M_3' >$, where $M_2' = h(ID_U||X) \oplus r_U'$ and $M_3' = g^{r_U'} \bmod p$. Then, he can replay the message and sends the message $< ID_U, M_2', M_3' >$ to server.

- On receiving the message $< ID_U, M_2, M_3 >$, S verifies the ID_U format. The validation holds, as the message is originally generated by user. Then, S computes $M_4 = h(ID_U||X)$ and $r_U' = M_2 \oplus M_4$, then verifies $M_3 = ? \ g^{r_U'} \bmod p$. The verification holds, as $r_U' = r_U$.
- S generates r_S and computes $M_5 = M_4 \oplus r_S$ and $M_6 = g^{r_S} \bmod p$, then sends the message $< M_5, M_6 >$ to U. S also computes session key $sk = (g^{r_U})^{r_S} \bmod p$.

5.4 Man-in-the Middle Attack

Without loss of generality, let the attacker has achieved previously transmitted message $< ID_U, M_2', M_3' >$ and $< M_5', M_6' >$, where $M_2' = h(ID_U||X) \oplus r_U'$, $M_3' = g^{r_U'} \bmod p$, $M_5' = h(ID_U||X) \oplus r_S'$ and $M_6' = g^{r_S'} \bmod p$. Then, he can perform the man-in-the middle attack as follows:

- When U sends the login message $< ID_U, M_2, M_3 >$ to S. E does not intercept U's message.
- On receiving the message $< ID_U, M_2, M_3 >$, S verifies the ID_U format. The validation holds, as the message is originally generated by user. Then, S computes $M_4 = h(ID_U||X)$ and achieves $r_U = M_2 \oplus M_4$, then verifies $M_3 =? g^{r_U} \bmod p$.
- S generates r_S and computes $M_5 = M_4 \oplus r_S$ and $M_6 = g^{r_S} \bmod p$. Then, it computes the session key $sk_{US} = (g^{r_U})^{r_S} \bmod p$.
- When S sends the message $< M_5, M_6 >$ to U. E intercepts S's message and replaces it with a old message $< M_5', M_6' >$.
- Upon receiving the message $< M_5', M_6' >$, the smart card computes $r_S' = M_1 \oplus M_5'$ and get r_S'. It verifies $M_6' =? g^{r_S'} \bmod p$. The verification holds, since $M_6' = g^{r_S'} \bmod p$. Then, smart card computes the session key $sk_{SU} = (g^{r_S'})^{r_U'} \bmod p$.

Both user and server agreed upon a session key, which are not equal, that is, $sk_{SU} \neq sk_{US}$, since $r_S \neq r_S'$ and $r_U \neq r_U'$. Therefore, user and server can not communicate with each other using the session key.

5.5 User Anonymity

In An's scheme, user real identity is associated with the login message, which reveals user's information to the attacker. This shows that An's scheme does not ensure user anonymity.

5.6 Inefficient Login Phase

In An's scheme, smart card does not verify the correctness of password in login phase.

Case 1

If a user inputs wrong password due to mistake. The smart card executes the login phase, which works as follows:

- When U inputs incorrect password PW_U^* instead of PW_U, the smart card does not verify the correctness of input and computes $J^* = h(PW_U^* \oplus N)||f$ and achieves M_1^* as:

$$M_1^* = e \oplus J^* = h(ID_U||X) \oplus J \oplus J^* = h(ID_U||X) \oplus (h(PW_U \oplus N)||f) \oplus (h(PW_U^* \oplus N)||f).$$

- The smart card generates a random number r_U, then computes $M_2 = M_1^* \oplus r_U$ and $M_3 = g^{r_U} \bmod p$. Finally, U sends the login message $< ID_U, M_2, M_3 >$ to S.

– S verifies the ID_U format. If ID_U is valid, S computes $M_4 = h(ID_U||X)$ and then r'_U as follows:

$$\begin{aligned} r'_U &= M_2 \oplus M_4 \\ &= M_1^* \oplus r_U \oplus M_4 \\ &= h(ID_U||X) \oplus (h(PW_U \oplus N)||f) \oplus (h(PW_U^* \oplus N)||f) \oplus r_U \oplus h(ID_U||X) \\ &= (h(PW_U \oplus N)||f) \oplus (h(PW_U^* \oplus N)||f) \oplus r_U \end{aligned}$$

Then verifies $M_3 =?\ g^{r'_U} \bmod p$. The verification does not hold, as $r'_U \neq r_U$.
– S terminates the session, as authentication does not hold.

Case 2:
If an attacker E intercepts U's login message, as an attacker can intercept the message. Then, the following steps executes:

– E intercepts the login message and replaces it with $< ID_U, M'_2, M_3 >$, where $M'_2 = M_2 \oplus r_E$ for random value r_E, i.e., $M'_2 = M_1 \oplus r_U \oplus r_E$.
– On receiving the message $< ID_U, M'_2, M_3 >$, S verifies the ID_U format. The validation holds, as the message includes user's original identity. Then, S computes $M_4 = h(ID_U||X)$ and achieves $r'_U = M'_2 \oplus M_4$, then verifies $M_3 =?\ g^{r'_U} \bmod p$. The verification does not hold, since $r'_U = r_U \oplus r_E$ instead of r_U.
– S terminates the session, as authentication does not hold.

In **case 1**, in spite of wrong password the smart card executes the login session. However, server terminates the session. Moreover, in case of message impersonation attack (**case 2**), the server also terminates the session in same step. Therefore, if the session terminates, it will be difficult for user to identify that exactly why the session is terminated.

6 Proposed Scheme

In this section, we present an improved scheme to overcome the weaknesses of An's schemes. The proposed scheme adopts three factor authentication. It has similar phases like Li and Hwang's scheme. In proposed scheme, a user first registers himself and achieves the smart card. Then, with the help of smart card he can login to the system and establish the session. The four phases of the proposed scheme are as follows: (i) Registration; (ii) Login; (iii) Verification; Password change.

Initially, the system chooses the large prime number p of bit size 1024, prime divisor q of $(p-1)$ of bit size 160. And, let g be a primitive element of order q in the finite field $GF(q)$, $h(\cdot)$ is a one way hash function, for example SHA-1. Then, server chooses its private key X and computes public key $Y = g^X \bmod p$.

6.1 Registration Phase

When a user wishes to register with the server to get the smart card, which works as follows:

Step R1. U selects his identity ID_U and chooses a password PW_U of his choice, then computes $W = h(PW_U||N)$, where N is a random number. Then, U imprints his personal biometric B_U at the fuzzy extractor, then the fuzzy extractor calculates $Gen(B_U) = (R_U, P_U)$, where R_U is an extracted string and P_U is a helper string. Finally, he submits ID_U and W with registration request to S via secure channel.

Step R2. Upon receiving the U's registration request, S verifies the legitimacy of ID_U. If this is invalid, it terminates the session. Otherwise, it computes $H = h(ID_U||X)$ and then $e = H \oplus W$. S embeds the values $\{e, h(\cdot), p, g, Y\}$ into the smart card and then returns the smart card to U.

Step R4. Upon receiving the smart card, U computes $L = N \oplus R_U$ and $V = h(ID_U||PW_U||N)$. Then, he stores P_U, L and V into the smart card.

6.2 Login Phase

When user wishes to login to the server, he inserts his smart card into card reader and inputs the identity ID'_U, password PW'_U and imprints his biometric B'_U at fuzzy extractor, then fuzzy extractor outputs $R'_U = Rep(B'_U; P_U)$. Note that $R_C = R'_C$, if B'_C is reasonably close to B_C. Upon getting the inputs, the smart card executes the login session as follows:

Step L1. Compute $N' = L \oplus R'_U$ and verify $V =?h(ID'_U||PW'_U||N')$. If verification does not hold, it terminates the session. Note that the verification holds, if user enters correct identity ($ID'_U = ID_U$) and password ($PW'_U = PW_U$), and imprints biometric B'_U is reasonably close to B_U. Otherwise, goto **Step L2.**

Step L2. Compute $H = e \oplus h(PW_U||N)$, select a random number r_U and then compute $A_1 = g^{r_U} \bmod p$, $A_2 = Y^{r_U} \bmod p = (g^X)^{r_U} \bmod p$, $NID = ID_U \oplus A_2$ and $C_U = h(ID_U||H||A_1||A_2||T_1)$, then send the login message $< NID, A_1, C_U, T_1 >$ to S, where T_1 is the U's current timestamp.

6.3 Verification Phase

User and server perform the following steps to mutually authenticate each other:

Step R1. On receiving the message $< NID, A_1, C_U, T_1 >$ at time T_2, S verifies $T_2 - T_1 \leqslant \Delta t$, where Δt is the valid time delay in message transmission. If verification does not hold, S terminates the session. Otherwise, it computes $A_3 = (g^{r_U})^X \bmod p$ and achieves $ID_U = NID \oplus A'_2$. Then, it computes $H = h(ID_U||X)$ and verifies $C_U =?\ h(ID_U||H||A_1||A_3||T_1)$. If verification does not hold, terminate the session. Otherwise, U is authenticated by S, then *Step R2* executes.

Step R2. S chooses a random number r_S and computes $A_4 = g^{r_S} \bmod p$, $A_5 = (g^{r_U})^{r_S} \bmod p$ and the session key $sk_{US} = h(ID_U||A_3||A_5||H||T_1||T_3)$, where T_3 is the current timestamp of S. Finally, it sends the message $< C_S, A_4, T_3 >$ to U, where $C_S = h(ID_U||sk_{US}||H||T_3)$.

Step R3. Upon receiving S's message $< C_S, A_4, T_3 >$ at time T_4, smart card verifies $T_4 - T_3 \leqslant \Delta t$. If time delay in message transmission is invalid, terminates the session. Otherwise, smart card achieves $A_6 = (g^{r_S})^{r_U} \bmod p$ and then the session key $sk_{SU} = h(ID_U||A_2||A_6||H||T_1||T_3)$. Finally, it verifies $C_S =? h(ID_U||sk_{SU}||H||T_3)$. If verification does not hold, terminate the session. Otherwise, S is authenticated by U, then U accepts sk_{SU} as the session key.

The agreed session key $sk_{US} = sk_{SU}$, as $A_2 = A_3$ and $A_5 = A_6$.

6.4 Password Change Phase

A user with old password and smart card can change the password as follows:

Step P1. U inserts his smart card into the card reader and inputs ID'_U, old password PW'_U, a new password PW_{new} and imprints his biometric B'_U at fuzzy extractor, then fuzzy extractor outputs $R'_U = Rep(B'_U; P_U)$.

Step P2. Smart card achieves $N = L \oplus R'_U$ and verifies $V =? h(ID'_U||PW'_U||N)$. If verification does not hold, terminates the session. Otherwise, smart card computes $e_{new} = e \oplus h(PW_U||N) \oplus h(PW_{new}||N)$ and $V_{new} = h(ID_U||PW_{new}||N)$. Then, it replaces e with e_{new} and V with V_{new}.

7 Security Analysis

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

Proposition 1. The proposed scheme preserves user anonymity.
Proof. In the proposed scheme, login message includes user dynamic identity $NID = ID_U \oplus A_2$, where $A_2 = g^{XR_U} \bmod p$. The computation $g^{XR_U} \bmod p$ for given $g^{r_U} \bmod p$ and $g^X \bmod p$ is equivalent to Diffie-Hellman problem, which is intractable. Therefore, ID_U can not be achieved from NID. Moreover, NID is different for each session , as user selects r_U randomly for each session. This makes A_2 different and so NID for each session. The different NID for different session, reduces the possibility of linkability. The unlinkability and dynamic identity concept, ensures user anonymity in the proposed scheme.

Proposition 2. The proposed scheme withstands offline password guessing attack.
Proof. In proposed scheme, to verify the correctness of guessed password, an adversary can use following conditions $V = h(ID_U||PW_U||N)$ and $e = H \oplus h(PW_U||N)$, where $N = L \oplus R_U$. Each condition involves N, to achieve N, user

biometric information is needed as $N = L \oplus R_U$. However, biometric information is user secret and unique information. Therefore, an attacker can not perform password guessing attack.

Proposition 4. The proposed scheme resists stolen smart card attack.
Proof. An attacker can extract the stored parameters $\{e, h(\cdot), p, g, Y, L, V\}$ of smart card. However, to generate a valid login message $< NID, A_1, C_U, T_1 >$, user's identity ID_U and user's long term key $H = h(ID_U||X)$ are needed. The identity is neither stored in smart card nor attached with any message. The login message includes, user's dynamic identity $NID = ID_U \oplus A_2$, where computation $A_2 = g^{XR_U} \bmod p$ for given $g^{r_U} \bmod p$ and $g^X \bmod p$ is equivalent to Diffie-Hellman problem. Therefore, identity can not be achieved from login message. Additionally, the stored value $V = h(ID_U||PW_U||N)$ includes ID_U, but in this expression ID_U is hashed with password. Therefore, ID_U can not even be guessed.

On the other hand, the secret values $H = h(ID_U||X)$ XORed with $h(PW_U||N)$, i.e., $e = H \oplus h(PW_U||N)$. Therefore, to achieve H, password PW_U and N are needed, where N is protected with biometric and password is secret. Therefore, an attacker can not achieve user long term secret H.

Proposition 5. The proposed scheme achieves known key secrecy.
Proof. In proposed scheme, the agreed session key $sk_{US} = h(ID_U||A_3||A_5||H||T_1||T_3)$ does not reveal any information about other session keys because:

1. Each key is hashed with one way hash function, therefore, no information can be drawn from the session key.
2. Each session key involves random numbers and the timestamps, which guarantees unique key for each session.
3. To construct a session key, user's secret key is needed, which is protected by password.

Proposition 6. The proposed scheme is efficient to resist stolen verifier attack.
Proof. In proposed scheme, the server does not maintain any verification table, therefore, stolen verifier attack will not work in proposed scheme.

Proposition 7. The proposed scheme achieves perfect forward secrecy.
Proof. If user's long term key H is compromised, then an attacker can not construct key $sk_{SU} = h(ID_U||A_2||A_6||H||T_1||T_3)$, as to construct the session key the values $A_2 = g^{XR_U} \bmod p$ and $A_6 = (g^{r_S})^{r_U} \bmod p$ are needed. To compute $(g^{r_S})^{r_U} \bmod p$ for given $g^{r_S} \bmod p$ and $g^{r_U} \bmod p$, which is equivalent to computational Deffie-Helman problem. And, the computation $g^{XR_U} \bmod p$ for given $g^{r_U} \bmod p$ and $g^X \bmod p$ is also equivalent to Diffie-Hellman problem. Therefore, with the knowledge of user long term key, an attacker can not construct established session key.

Proposition 8. The proposed scheme resists Known session-specific temporary information attack.

Proof. If temporary secret r_U and r_S are compromised, then an attacker can construct $A_2 = g^{XR_U} \bmod p$ and $A_6 = (g^{r_S})^{r_U} \bmod p$. However, to compute the session key $sk_{SU} = h(ID_U||A_2||A_6||H||T_1||T_3)$, the user long term secret key $H = h(ID_U||X)$ is needed, which is protected with password.

Proposition 9. The proposed scheme forbids replay attack.
Proof. Time stamps are considered to be the counter measures to resist the replay attack [25, 26]. An attacker can not replay the message in the proposed scheme, as each transmitted message includes the time stamp. And, if the receiver finds the time delay in message transmission, he immediately terminates the session. Moreover, an attacker can not construct a new message, since a valid message includes message authentication codes M_U or M_S, where to construct them, user's secret key H is needed. Since the user's secret key is secured, the replay attack will not work.

Proposition 10. The proposed scheme ensures key freshness property.
Proof. Each session key involves random numbers and timestamp, where timestamps are unique for each session. Uniqueness property for different sessions guaranties the unique key for each session. The unique key construction for each session ensures the key freshness property.

Proposition 11. The proposed scheme achieves mutual authentication.
Proof. In mutual authentication mechanism, user must prove its identity to the server and server must prove its identity to user. In proposed scheme, user and server both authenticate each other. To achieve it, user and server exchange message authentication codes, which include entities identities and secret keys. To forge user or server, secret value H is needed, which is protected with the password. In authentication phase, server verifies user authenticity by $C_U =?h(ID_U||H||A_1||A_3||T_1)$ and user verifies by $C_S =?\ h(ID_U||sk_{SU}||H||T_3)$, where C_S and C_U both involve secret key H.

Proposition 12. The proposed scheme presents efficient login and password change phase.
Proof. Upon getting the inputs, identity ID_U, biometric B_U and password PW_U, the smart card achieves $N = L \oplus R_U$ and then verifies $V =?\ h(ID_U||PW_U||N)$. If verification does not hold, terminate the session. Since the condition $V =?\ h(ID_U||PW_U||N)$ involves user's identity, password, and a random value which can only be achieved when imprints biometric B'_U is reasonably close to B_U. Therefore, if user enters any of the values incorrect, the session terminates. This shows that login and password change phases are efficient to track incorrect login.

8 Conclusion

The presented article analyzes Li et al.'s and An's biometric based remote user authentication schemes and demonstrates the weaknesses of both the schemes.

This investigation shows that both the scheme are inefficient to present three-factor remote user authentication. Moreover, both the schemes do not provide efficient login phase and fail to preserve user anonymity. Further, the article presents an improved anonymous remote user authentication scheme. It overcomes all the weaknesses of Li et al.'s and An's schemes. Moreover, proposed scheme presents efficient login and password change mechanism where incorrect input is quickly detected and user can freely change his password.

References

1. Li, X., Niu, J., Khurram Khan, M., Liao, J.: An enhanced smart card based remote user password authentication scheme. Journal of Network and Computer Applications (2013)
2. Jaspher, G., Katherine, W., Kirubakaran, E., Prakash, P.: Smart card based remote user authentication scheme–survey. In: 2012 Third International Conference on Computing Communication & Networking Technologies (ICCCNT), pp. 1–5. IEEE (2012)
3. Xu, J., Zhu, W.T., Feng, D.G.: An improved smart card based password authentication scheme with provable security. Computer Standards & Interfaces 31(4), 723–728 (2009)
4. Messerges, T.S., Dabbish, E.A., Sloan, R.H.: Examining smart-card security under the threat of power analysis attacks. IEEE Transactions on Computers 51(5), 541–552 (2002)
5. Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)
6. Das, A.: Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards. Information Security, IET 5(3), 145–151 (2011)
7. Wang, D., Ma, C.G.: Cryptanalysis and security enhancement of a remote user authentication scheme using smart cards. The Journal of China Universities of Posts and Telecommunications 19(5), 104–114 (2012)
8. Wen, F., Li, X.: An improved dynamic id-based remote user authentication with key agreement scheme. Computers & Electrical Engineering 38(2), 381–387 (2012)
9. Li, X., Niu, J., Wang, Z., Chen, C.: Applying biometrics to design three-factor remote user authentication scheme with key agreement. Security and Communication Networks (2013)
10. Lee, C.C., Chang, R.X., Chen, L.A.: Improvement of li-hwang's biometrics-based remote user authentication scheme using smart cards. WSEAS Transactions on Communications 10(7), 193–200 (2011)
11. Truong, T.T., Tran, M.T., Duong, A.D.: Robust biometrics-based remote user authentication scheme using smart cards. In: 2012 15th International Conference on Network-Based Information Systems (NBiS), pp. 384–391. IEEE (2012)
12. An, Y.: Security analysis and enhancements of an effective biometric-based remote user authentication scheme using smart cards. In: BioMed Research International 2012 (2012)
13. 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. Journal of Network and Computer Applications 34(1), 73–79 (2011)

14. Li, C.T., Hwang, M.S.: An efficient biometrics-based remote user authentication scheme using smart cards. Journal of Network and Computer Applications 33(1), 1–5 (2010)
15. Chang, Y.F., Yu, S.H., Shiao, D.R.: A uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care. Journal of Medical Systems 37(2), 1–9 (2013)
16. Lee, T.F., Chang, I.P., Lin, T.H., Wang, C.C.: A secure and efficient password-based user authentication scheme using smart cards for the integrated epr information system. Journal of Medical Systems 37(3), 1–7 (2013)
17. Go, W., Lee, K., Kwak, J.: Construction of a secure two-factor user authentication system using fingerprint information and password. Journal of Intelligent Manufacturing, 1–14 (2012)
18. An, Y.: Improved biometrics-based remote user authentication scheme with session key agreement. In: Kim, T.-H., Cho, H.-S., Gervasi, O., Yau, S.S. (eds.) GDC/IESH/CGAG 2012. 351, vol. CCIS, pp. 307–315. Springer, Heidelberg (2012)
19. 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: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 203–220. Springer, Heidelberg (2008)
20. Cheng, Z., Nistazakis, M., Comley, R., Vasiu, L.: On the indistinguishability-based security model of key agreement protocols-simple cases. In: Proc. of ACNS, Citeseer, vol. 4 (2004)
21. Blake-Wilson, S., Johnson, D., Menezes, A.: Key agreement protocols and their security analysis. Springer (1997)
22. Blake-Wilson, S., Menezes, A.: Authenticated diffe-hellman key agreement protocols. In: Tavares, S., Meijer, H. (eds.) SAC 1998. LNCS, vol. 1556, pp. 339–361. Springer, Heidelberg (1999)
23. Menezes, A.J., Van Oorschot, P.C., Vanstone, S.A.: Handbook of applied cryptography. CRC Press (2010)
24. Aura, T.: Strategies against replay attacks. In: Proceedings of the 10th Computer Security Foundations Workshop 1997, pp. 59–68. IEEE (1997)
25. Zhen, J., Srinivas, S.: Preventing replay attacks for secure routing in ad hoc networks. In: Pierre, S., Barbeau, M., An, H.-C. (eds.) ADHOC-NOW 2003. LNCS, vol. 2865, pp. 140–150. Springer, Heidelberg (2003)
26. Malladi, S., Alves-Foss, J., Heckendorn, R.B.: On preventing replay attacks on security protocols. Technical report, DTIC Document (2002)
27. Juang, W.S., Lei, C.L., Chang, C.Y.: Anonymous channel and authentication in wireless communications. Computer Communications 22(15), 1502–1511 (1999)
28. Chang, C.C., Lee, C.Y., Chiu, Y.C.: Enhanced authentication scheme with anonymity for roaming service in global mobility networks. Computer Communications 32(4), 611–618 (2009)
29. Xu, J., Zhu, W.T., Feng, D.G.: An efficient mutual authentication and key agreement protocol preserving user anonymity in mobile networks. Computer Communications 34(3), 319–325 (2011)
30. Wang, R.C., Juang, W.S., Lei, C.L.: Robust authentication and key agreement scheme preserving the privacy of secret key. Computer Communications 34(3), 274–280 (2011)
31. Khan, M.K., Kim, S.K., Alghathbar, K.: Cryptanalysis and security enhancement of a more efficient & secure dynamic id-based remote user authentication scheme. Computer Communications 34(3), 305–309 (2011)