Journal of King Saud University – Computer and Information Sciences (2017) **29**, 54–62

King Saud University

Journal of King Saud University – Computer and Information Sciences

www.ksu.edu.sa
www.sciencedirect.com

An enhanced dynamic ID-based authentication scheme for telecare medical information systems

Ankita Chaturvedi, Dheerendra Mishra *, Sourav Mukhopadhyay

Department of Mathematics, Indian Institute of Technology Kharagpur, Kharagpur 721302, India

Received 25 August 2014; revised 24 October 2014; accepted 9 December 2014
Available online 7 November 2015

KEYWORDS

Telemedicine;
Password based authentication;
Smart card;
Security;
Privacy

Abstract The authentication schemes for telecare medical information systems (TMIS) try to ensure secure and authorized access. ID-based authentication schemes address secure communication, but privacy is not properly addressed. In recent times, dynamic ID-based remote user authentication schemes for TMIS have been presented to protect user's privacy. The dynamic ID-based authentication schemes efficiently protect the user's privacy. Unfortunately, most of the existing dynamic ID-based authentication schemes for TMIS ignore the input verifying condition. This makes login and password change phases inefficient. Inefficiency of the password change phase may lead to denial of service attack in the case of incorrect input in the password change phase. To overcome these weaknesses, we proposed a new dynamic ID-based authentication scheme using a smart card. The proposed scheme can quickly detect incorrect inputs which makes the login and password change phase efficient. We adopt the approach with the aim to protect privacy, and efficient login and password change phases. The proposed scheme also resists off-line password guessing attack and denial of service attack. We also demonstrate the validity of the proposed scheme by utilizing the widely-accepted BAN (Burrows, Abadi, and Needham) logic. In addition, our scheme is comparable in terms of the communication and computational overheads with relevant schemes for TMIS.
© 2015 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

1. Introduction

The omnipresence and easy access of the Internet, provides a scalable platform for healthcare services. One of the popular health care services is telecare medical information systems (TMIS) which supports healthcare delivery services to the patients' homes. As we are moving from paper based health records to electronic health records, the TMIS offers an easy access of electronic records to remote users. TMIS is making a difference by employing information and communication technologies to enhance the quality of healthcare related services in the management of chronic diseases.

Increasing computation power has made the adversary powerful enough so that he can control communications over the public network (Aloul et al., 2009a; Mishra et al., 2014a; Alfantookh, 2006). Thus, authorized communication is required to ensure in TMIS. To reduce the adversary threat,

* Corresponding author.
E-mail address: dheerendra@maths.iitkgp.ernet.in (D. Mishra).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jksuci.2014.12.007
1319-1578 © 2015 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

smart card based authentication schemes are designed and developed (Aloul et al., 2009b; Mishra et al., 2014b; Al-Muhtadi, 2007), which goal is to address the following attributes:

One time registration: It allows the patient to register once with the medical server and then he can access the services any number of times.
Efficient login phase: A login phase should be capable of detecting incorrect login inputs. In other words, smart card should not execute the login session in the case of wrong identity or password input.
Efficient password change phase: The scheme should be able to quickly detect incorrect inputs in the password change phase.
User-friendly password change phase: A user should be allowed to change his password input and only allows a patient to update his password freely without the medical server's assistance.
Mutual authentication and session key agreement: It allows a patient and medical servers to mutually authenticate each other and establish a common key, which should be constructed with the equal participation of both the user and server.
Security attributes: The smart card based authentication scheme must be able to withstand man-in-the middle attack, impersonation attack, guessing attack, insider attack, replay attack, stolen smart card attack and known session-specific temporary information attack. Moreover, the scheme should support session key agreement, key freshness property, mutual authentication and forward secrecy.

Wu et al. (2012) introduced an efficient authentication scheme for TMIS, which is better than the previously proposed schemes for low computing devices by adding the pre-computing phase. In the pre-computing phase, the user performs an exponential operation, and then stores the calculated values into the storage device such that a user can extract these values from the device whenever he requires. However, He et al. (2012) demonstrated that Wu et al.'s scheme fails to resist an impersonation attack. They also introduced an enhanced scheme and claimed that their proposed scheme eliminates the drawbacks of Wu et al.'s scheme. They also claimed that their scheme is more appropriate for low power mobile devices for TMIS. Although Wei et al. (2012) identified that both Wu et al.'s and He et al.'s schemes are inefficient to meet two-factor authentication, whereas an efficient password based authentication scheme using a smart card should achieve two-factor authentication. They also presented an improved smart card based authentication scheme for TMIS to ensure two-factor authentication. In 2012, Zhu (2012) demonstrated that Wei et al.'s scheme is vulnerable to off-line password guessing attack. He also presented an improved scheme for TMIS and claimed that his scheme could overcome the weaknesses of Wei et al.'s scheme. However, his scheme does not protect anonymity which enables an adversary to track the consumer's current location and login history (Mishra and Mukhopadhyay, 2014). Although consumer's anonymity during message exchange ensures consumer's privacy by preventing an attacker from acquiring a consumer's sensitive personal information.

Chen et al. (2012) proposed a dynamic ID-based authentication scheme for TMIS which protects user anonymity and has less computation overhead. However, in 2013, Lin (2013) demonstrated that user identity is compromised under the dictionary attack and the password can be derived with the stolen smart card in Chen et al's scheme. He also proposed an improved scheme which efficiently resists dictionary attack and protects anonymity. Unfortunately, Lin's scheme does not include the input verifying condition. This makes login and password change phases inefficient. The inefficiency of the login phase causes extra communication and computation overhead. The inefficient password change phase in Lin's scheme causes denial of service attack (DOS) in the case of incorrect input in password change (Mishra, 2015b). The DOS attack does not allow an authorized user to access the resources (Alfantookh, 2006). Xie et al. (2013) showed that Chen et al.'s scheme is vulnerable to an impersonation attack and off-line password guessing attack using a stolen smart card. Additionally, they presented an improved scheme for TIMS to overcome the weaknesses of Chen et al.'s scheme. However, Xie et al.'s scheme also failed to present an efficient login and password change phase (Mishra, 2015b). Cao and Zhai (2013) demonstrated that Chen et al's scheme is vulnerable to an off-line identity guessing attack and undetectable on-line password guessing attack using a stolen smart card. They also proposed an improved authentication scheme to resist guessing attacks. Their scheme efficiently protects anonymity and password guessing attack, but does not present an efficient login phase and has an unfriendly password change phase (Mishra, 2015b). The smart card cannot identify the correctness of the input in the above discussed schemes (Lin, 2013; Wei et al., 2012; Xie et al., 2013; Zhu, 2012; Xu et al., 2014; Lee et al., 2013; Jiang et al., 2014) which either causes DOS attack or makes the password chance phase unfriendly. The schemes (Lin, 2013; Wei et al., 2012; Xie et al., 2013; Zhu, 2012; Xu et al., 2014; Lee et al., 2013; Jiang et al., 2014) present an inefficient password change phase (Mishra, 2015b; Mishra, 2015a) and the schemes (Cao and Zhai, 2013; Jiang et al., 2013; Wu and Xu, 2013) have an unfriendly password change phase as every time before changing the password the user has to establish an authorized session with the server, that is, user cannot independently change his/her password in these schemes. More detailed characterization of security attributes of the schemes (Wei et al., 2012; Zhu, 2012; Lee et al., 2013; Chen et al., 2012; Cao and Zhai, 2013; Xie et al., 2013; Lin, 2013; Xu et al., 2014) is presented in Table 1.

Motivation: Many of the schemes (Lin, 2013; Wei et al., 2012; Xie et al., 2013; Zhu, 2012; Xu et al., 2014; Lee et al., 2013) cannot identify the correctness of input which leads to a denial of service scenario in the case of incorrect input in the password change phase (Mishra, 2015a,b). A single mistake in the password change phase does not allow a user to login to the server using the same smart card. In other words, an authorized user can never use the smart card to login to the server if he/she commits a mistake in password change. It is a serious security pitfall as user's may himself/herself cause denial of service attack. In general, a user cannot be considered an expert who never commits a mistake. It is always be possible that a human may sometimes forget the password or commit a mistake while entering the password. Moreover, a user may have several accounts and may use different passwords

Table 1 Security attributes comparison of some recent password based authentication schemes for TMIS.

Security attributes	Schemes							
	Wei et al. (2012)	Zhu (2012)	Lee et al. (2013)	Chen et al. (2012)	Cao and Zhai (2013)	Xie et al. (2013)	Lin (2013)	Xu et al. (2014)
User anonymity	×	×	√	√	√	√	√	√
Insider attack	√	√	√	√	√	√	√	√
Off-line password guessing attack	×	√	√	×	√	√	√	√
Replay attack	√	√	√	√	×	√	√	√
Session key agreement	√	×	√	√	√	√	√	√
Session key verification	√	–	√	×	√	×	×	√
Efficient password change phase	×	×	×	√	√	×	×	×
Denial of service attack	×	×	×	√	√	×	×	×
User-friendly password change phase	×	×	×	√	×	√	√	√
Efficient login	×	×	×	√	×	×	×	×

for different accounts; in that case it is also possible to use one account password in another account by mistake. Thus, the mistake in the password change phase should not affect the outcome the denial of service attack. In order to overcome this drawback, efficient authentication schemes should be able to quickly detect incorrect inputs so that the denial of service scenario can be avoided for authorized users.

Our contributions: In this article, we propose an improved scheme with the aim to achieve an efficient login phase and password change phase. The proposed scheme protects the user's privacy and resists guessing attack. Moreover, we demonstrate the validity of the proposed scheme through the BAN (Burrows, Abadi, and Needham) logic.

Organization of the article: The rest of the article is sketched as follows: The proposed password based authentication scheme for TMIS is presented in Section 2. Section 3 presents the security analysis. Section 4 discuss the comparative performance of the proposed scheme. Finally, the conclusion is drawn in Section 5.

2. Proposed password based authentication scheme

In this section, we propose an improved scheme to ensure efficient authorized communication. The proposed scheme is designed with the aim to provide an anonymous and efficient authentication phase. In this scheme, a new user first completes his registration with the server, and achieved a personalized smart card. Then, the registered user can establish an authorized session with the server. The scheme comprises of four phases, namely, registration, login, authentication and password change. The notations used in the proposed scheme are given in Table 2.

2.1. Registration phase

The server S generates two large primes p and q of 512-bits and computes $N = pq$ of 1024-bits modulus. S also chooses a prime number e and an integer d such that $ed \equiv 1 \bmod (p-1)(q-1)$. S keeps p, q and d secret, and makes N and e public. Then a new user U can register to the server and achieve a personalized smart card as follows:

Step 1. User U chooses a password of his choice and a random number b. U computes $W = h(PW_U||b)$ and submits the registration request with a message $\langle ID_U, W \rangle$ to S via secure channel.

Step 2. Upon receiving the U's request, S verifies whether ID_U is previously registered or not. If ID_U is already registered, S asks for a new identity. Otherwise, S computes $H = h(d \oplus ID_U)$ and $v = W \oplus H$. Then S personalizes smart card SC by embedding the parameters $\{N, v, e, h(\cdot)\}$ and returns SC to U via secure channel. S stores ID_U in registered users' database.

Step 3. U computes $H = v \oplus W, A = b \oplus h(ID_U||PW_U)$ and $B = h(b||H||h(ID_U||PW_U))$. Then U stores A and B into the smart card (see Fig. 1).

2.2. Login phase

A register user with a valid smart card generates the login message and sends the login message to the server as follows:

Table 2 Meaning of symbols used throughout the paper.

Notation	Descryption
S	A trustworthy server
p, q	Two large primes
N	Product of p and q
Z_N	Ring of integers modulo N
e	Public key of S
d	Private/secret key of S
E	Adversary/attacker
SC	Smart card
U	User/patient
ID_U	Identity of U
PW_U	Password of U
$h(\cdot)$	A collision resistant one-way hash function
$\oplus$	XOR
$\|\|$	String concatenation operation
ΔT	Valid time delay in message transmission

Step 1. User U inserts his smart card SC into the card reader and inputs ID_U and PW_U.

Step 2. SC computes $b = A \oplus h(ID_U||PW_U), W = h(PW_U||b)$ and $H = v \oplus W$. SC verifies $B \stackrel{?}{=} h(b||H||h(ID_U||PW_U))$. If the verification does not hold, SC terminates the session. Otherwise, SC selects a random number r_u, and computes $R = h(ID_U||r_u||H||T_u)$ and $X = (ID_U||r_u||R)^e \bmod N$ where T_u is the current timestamp. SC sends the message $\langle X, T_u \rangle$ to S (see Fig. 2).

2.3. Authentication phase

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

Step 1. Upon receiving the message $\langle X, T_u \rangle$ at time T'_u, S verifies $T'_u - T_u \leqslant \Delta t$. If the verification holds, S computes $X^d \bmod N = (ID_U||r_u||R)$ and $H = h(d \oplus ID_U)$. S verifies $R \stackrel{?}{=} h(ID_U||r_u||H||T_u)$. If the verification holds, S considers U as an authorized user.

Step 2. S computes the session key $sk_{SU} = h(H \oplus r_u \oplus T_u \oplus T_s)$ and $Y = h(ID_U||sk_{SU}||H)$. Finally, S responds with the message $\langle Y, T_s \rangle$.

Step 3. Upon receiving the responder's message $\langle Y, T_s \rangle$ at time T'_s, SC checks whether the condition $(T'_s - T_s) \leqslant \Delta t$ holds. If the condition holds, SC computes session key $sk_{US} = h(H \oplus r_u \oplus T_u \oplus T_s)$. Then SC verifies $Y \stackrel{?}{=} h(ID_U||sk_{US}||H)$. If the verification holds, U considers sk_{US} as the session key and S as a authorized server (see Fig. 3).

2.4. Password change phase

A legal user U can change the password of the smart card without the server's assistance. To change the password, he inserts the smart card into the card reader, and inputs current password and identity. The smart card verifies the correctness of the current password and identity. If the verification holds, the smart card asks for a new password and then completes the password update. The description of password change phase is as follows:

Step 1. User U inputs PW_U and ID_U.

Step 1. The smart card SC computes $h(ID_U||PW_U)$ and achieves $b = A \oplus h(ID_U||PW_U), W = h(PW_U||b)$ and $H = v \oplus W$. SC verifies $B \stackrel{?}{=} h(b||H||h(ID_U||PW_U))$. If the verification does not hold, SC terminates the session. Otherwise, SC asks for a new password.

Step P2. User U enters new password PW_{new}.

Step P3. The smart card SC computes $W_{new} = h(PW_{new}||b)$, $v_{new} = H \oplus W_{new}, A_{new} = b \oplus h(ID_U||PW_{new})$, and $B_{new} = h(b||H||h(ID_U||PW_{new}))$. SC replaces A with A_{new}, B with B_{new}, and v with v_{new} (see Fig. 4).

3. Security analysis

In this section, we show how the proposed scheme satisfies desirable security attributes.

3.1. Authentication proof based on BAN logic

Some notations used in BAN logic analysis are described as follows:

$P| \equiv X$: The principal P believes the statement X.
$P \triangleleft X$: P sees X, means that P has received a message X.
$P| \sim X$: P once said X, means that $P| \equiv X$ when P sent it.
$P| \Rightarrow X$: P controls X, P has an authority on X (Jurisdiction over X).
$\sharp(X)$: The message X is fresh.
$P| \equiv Q \stackrel{K}{\leftrightarrow} P$: P and Q use K (shared key) to communicate with each other.
$P \stackrel{x}{\leftrightarrow} Q : x$ is a shared secret information between P and Q.
$\{X\}_K$: The formula X is encrypted under K.
$\langle X \rangle_Y$: The formula X is combined with formula Y.
$(X)_K$: The formula X is hashed with the key K.
$\stackrel{K}{\rightarrow} P : K$ is public key of P.
$P \stackrel{X}{\rightleftharpoons} Q : X$ is a secret formula, known only to P and Q.

In order to describe logical postulates of BAN logic in formal terms (Burrows et al., 1989; Syverson and Cervesato, 2001), we present the following rules:

Rule (1). Message meaning rule:

For shared secret keys:

$$\frac{P| \equiv Q \stackrel{K}{\leftrightarrow} P, P \triangleleft \{X\}_K}{P| \equiv Q| \sim X} \quad (1)$$

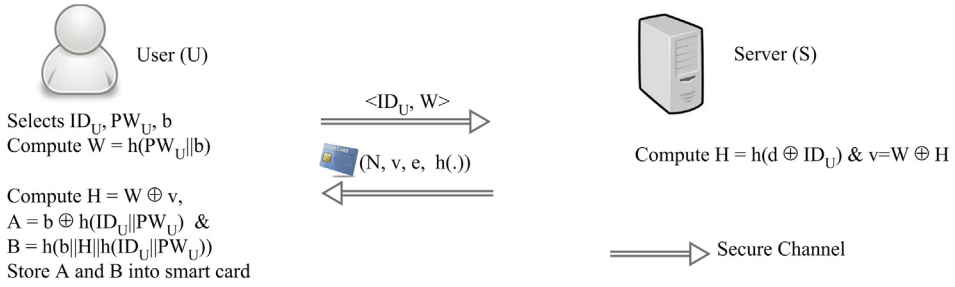

Figure 1 Registration phase: a new user U registers with his identity ID_U and achieve a personalized smart card with stored parameters $\{N, v, e, h(\cdot)\}$. U also stores A and B into the smart card.

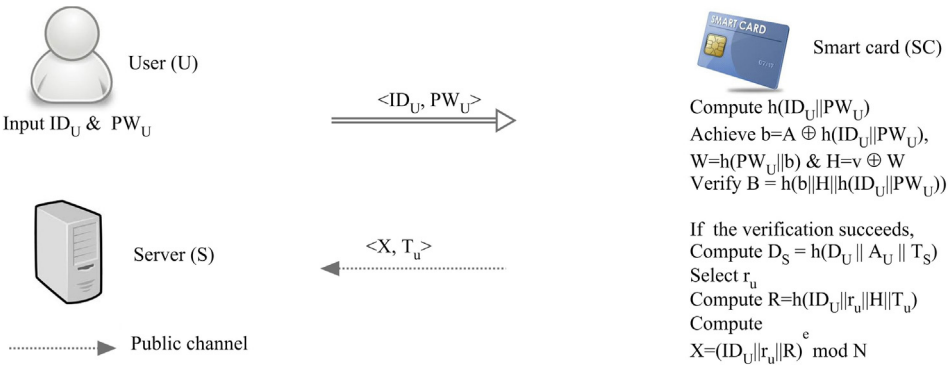

Figure 2 Login phase: a user U generates a login message $\langle X, T_u \rangle$ using the smart card, and sends it to server S.

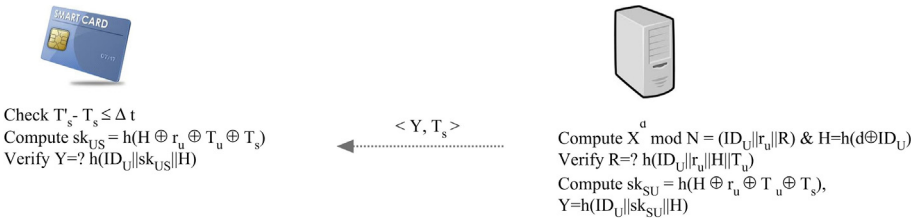

Figure 3 Authentication phase: user and server verify the authenticity of each other and draw a session key.

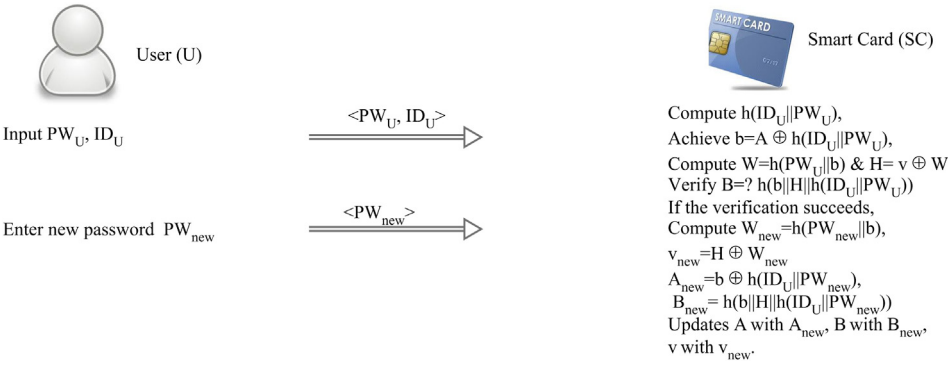

Figure 4 Password change phase: a user changes the password of the smart card without server assistance.

If P believes that K is shared with Q and sees X encrypted under k, then P believes that Q once said X.

Rule (2). The nonce verification rule:

$$\frac{P| \equiv \sharp(X), P| \equiv Q| \sim X}{P| \equiv Q| \equiv X} \tag{2}$$

If P believes that X has been uttered recently (freshness) and P believes that Q once said X, and then P believes that Q believes X.

Rule (3). The jurisdiction rule:

$$\frac{P| \equiv Q| \Rightarrow X, P| \equiv Q| \equiv X}{P| \equiv X} \tag{3}$$

If P believes that Q has jurisdiction over X, and P believes that Q believes a message X, then P believes X.

Rule (4). The freshness rule:

$$\frac{P| \equiv \sharp(X)}{P| \equiv \sharp(X, Y)} \tag{4}$$

If one part is known to be fresh, then the entire formula must be fresh.

According to the analytic procedures of the BAN logic, the proposed protocol will satisfy the following goals:

Goal 1. $U| \equiv (U \overset{SK}{\leftrightarrow} S)$;

Goal 2. $S| \equiv (U \overset{SK}{\leftrightarrow} S)$;

The protocol generic type:

Message 1. $U \rightarrow S : (ID_U||r_u||h(ID_U||r_u||H||T_u))^e mod N, T_u$

Message 2. $S \rightarrow U : h(ID_U||sk||H), T_s$

Idealize form of the protocol:

Message 1. $U \rightarrow S : \{ID_U, r_u, (ID_U, r_u, T_u)_H\}_e, T_u$

Message 2. $S \rightarrow U : (ID_U, U \overset{sk}{\leftrightarrow} S)_H, T_s$

We make the following assumptions about the initial state of the protocol to analyze the proposed protocol:

A1: $U| \equiv \sharp(T_u)$;
A2: $S| \equiv \sharp(T_s)$;
A3: $U| \equiv (U \overset{H}{\leftrightarrow} S)$;
A4: $S| \equiv (U \overset{H}{\leftrightarrow} S)$;
A5: $U| \equiv S| \equiv (U \overset{H}{\leftrightarrow} S)$;
A6: $S| \equiv U| \equiv (U \overset{H}{\leftrightarrow} S)$;

We analyze the idealized form of the proposed protocol based on the BAN logic rules and the assumptions. The main proofs are described as follows:

According to the message 1, we could get:

S_1: $S \triangleleft (ID_U, r_u, T_u)_H, T_u$

According to the assumption A4, we apply the message meaning rule to get:

S_2: $S| \equiv U| \sim T_u$

According to the assumption A1, we apply the freshness conjuncatenation rule to get:

S_3: $S| \equiv \sharp(ID_U, r_u T_u)_H$

According to the S_2 and S_3, we apply nonce verification rule to obtain

S_4: $S| \equiv U| \equiv (ID_U, r_u, T_u)_H$

According to the assumption A4 and S_4, we apply the jurisdiction rule to get:

S_5: $S| \equiv T_u$

According to $sk = h(H \oplus r_u \oplus T_u \oplus T_s), S_5$ and A2, we could obtain

S_6: $S| \equiv (U \overset{SK}{\leftrightarrow} S)$ **(Goal 2.)**

According to the message 2, we could obtain:

S_7: $U \triangleleft (ID_U, U \overset{sk}{\leftrightarrow} S)_H, T_s$

According to the assumption A3, we apply the message meaning rule to get:

S_8: $U| \equiv S| \sim T_s$

According to the assumption A2, we apply the freshness conjuncatenation rule to get:

S_9: $U| \equiv \sharp(ID_U, U \overset{sk}{\leftrightarrow} S)_H$

According to the S_8 and S_9, we apply nonce verification rule to obtain

S_{10}: $U| \equiv S| \equiv (ID_U, U \overset{sk}{\leftrightarrow} S)_H$

According to the assumption A3 and S_{10}, we apply the jurisdiction rule to get:

S_{11}: $U| \equiv T_s$

According to $sk = h(H \oplus r_u \oplus T_u \oplus T_s), S_{11}$ and A1, we could obtain

S_{12}: $U| \equiv (U \overset{SK}{\leftrightarrow} S)$ **(Goal 1.)**

3.2. Discussion on the possible attacks

3.2.1. User anonymity and unlinkability

The login message $\langle X, T_u \rangle$ is encrypted with the server's public key and includes user's identity along with random value r, i.e., $X = (ID_U || r_u || R)^e \bmod N$. As X is encrypted with the server's public key, no adversary can retrieve ID_U from X. Moreover, the smart card does not include the user's identity. Therefore, an adversary cannot identify the message source. The timestamp T_u is distinct for each session. This ensures distinct login messages for each session. Thus an adversary cannot link between any two login messages. Unlinkability and anonymity make communication completely private.

3.2.2. Insider attack

A malicious insider in the server's system may try to achieve the user's password. However, the user does not submit the password PW_U in its original form, *i.e.,* user submits $h(PW_U||b)$ instead of PW_U to the server. Therefore, a malicious insider cannot know the user's password PW_U as hash function $h(\cdot)$ cannot be reverted. Moreover, an adversary cannot perform the password guessing attack as the user does not submit b to S.

3.2.3. Efficient login phase

The smart card SC can identify the correctness of the input in the following cases as follows:

Case-1 If a user inputs an incorrect password PW_U^* and correct identity ID_U.

The smart card SC computes $h(ID_U||PW_U^*)$ and achieves $b^* = A \oplus h(ID_U||PW_U^*), W^* = h(PW_U^*||b^*)$ and $H^* = v \oplus W^*$. The smart card SC computes $B^* = h(b^*||H^*||h(ID_U||PW_U^*))$ and verifies $B \overset{?}{=} B^*$. The verification does not hold as $B \neq B^*$. Therefore, SC terminates the session.

Case-2 If a user inputs incorrect identity ID_U^* and correct password PW_U.

The smart card SC computes $h(ID_U^*||PW_U)$ and achieves $b'^* = A \oplus h(ID_U^*||PW_U), W'^* = h(PW_U||b'^*)$ and $H'^* = v \oplus W'^*$. The smart card SC computes $B'^* = h(b'^*||H'^*||h(ID_U^*||PW_U))$ and verifies $B \overset{?}{=} B'^*$. The verification does not hold as $B \neq B'^*$. Therefore, SC terminates the session.

Case-3 If a user inputs incorrect identity ID_U^* and incorrect password PW_U^*.

The smart card SC computes $h(ID_U^*||PW_U^*)$ and achieves $b''^* = A \oplus h(ID_U^*||PW_U^*), W''^* = h(PW_U^*||b''^*)$ and $H''^* = v \oplus W''^*$. The smart card SC computes $B''^* = h(b''^*||H''^*||h(ID_U^*||PW_U^*))$ and verifies $B \overset{?}{=} B''^*$. The verification does not hold as $B \neq B''^*$. Therefore, SC terminates the session.

In all the cases, smart card can efficiently detect the incorrect input and terminate the session. This shows that the proposed scheme has an efficient login phase.

3.2.4. User-friendly and efficient password changes phase

The user can change his password without the server's assistance. Moreover, the smart card verifies the correctness of inputs using the condition $B \overset{?}{=} h(b||H||h(ID_U||PW_U))$ which includes identity and password, and is similar to the login phase. As the login phase can efficiently verify the correctness of the input, the password change phase can also be efficient to detect the incorrect input.

3.2.5. Stolen smart card attack

An adversary can retrieve the parameters $\langle N, v, e, A, B \rangle$ from the stolen smart card and try to generate a valid login message using the achieved parameters. However, to construct the valid login message $\langle X, T_u \rangle$, is equivalent to achieve a user's long-term key H along with identity ID_U as $R = h(ID_U||r_u||H||T_u)$.

As H is protected with password PW_U, an adversary cannot use the stolen smart card to generate a valid login message.

3.2.6. Off-line password guessing attack

To succeed a password guessing attack, verification of the guessed password is necessary. The password is associated with the following values: $v = h(PW_U||b) \oplus h(d \oplus ID_U), A = b \oplus h(ID_U||PW_U)$ and $B = h(b||H||h(ID_U||PW_U))$. To verify the password using the expression $B = h(b||H||h(ID_U||PW_U))$, an adversary needs to achieve b and H. Although H cannot be achieved without knowing b as $H = v \oplus h(PW_U||b)$. Since $b = A \oplus h(ID_U||PW_U)$, to retrieve b, user identity ID_U is needed. Neither the smart card nor the transmitted message includes the user's identity. This shows that the proposed scheme resists the password guessing attack.

3.2.7. Replay attack

Replay attack is the most common attack in the authentication process. However, the common countermeasures are timestamp and random number. In the proposed scheme, the transmitted login message $\langle X, T_u \rangle$ includes timestamp. Moreover, to modify the message $\langle X' (= (ID_U||r_u||R')^e \bmod N), T_E \rangle$ using current timestamp T_E, an adversary has to compute $R' = h(ID_U||r_u||H||T_E)$. The computation of R' requires H along with ID_U. Since, H and ID_U are secret, an adversary cannot replay the previously transmitted messages.

3.2.8. User impersonation attack

An adversary E can masquerade as a legitimate user to login to the server. However, the proposed scheme can resist this attack as follows:

E can try to login to the server using replay attack. Although the proposed scheme resists the replay attack.
E can try to generate a valid login message $\langle X', T_E \rangle$ for a random value r_E and current timestamp T_E, where $X' = (ID_U||r_E||R')^e \bmod N$. To compute X', E has to compute R'. However, no unauthorized user can compute R' due to following facts:

- To compute R', user's secret key H and identity ID_U are needed as $R' = h(ID_U||r_E||H||T_E)$.
- Neither the smart card nor the transmitted messages includes ID_U. Thus, an adversary cannot achieve ID_U.
- To retrieve H from v, the password is needed. Since the password is only known to the user, an adversary cannot achieve H.

This shows that the proposed scheme resists user impersonation attack.

3.2.9. Server impersonation attack

An adversary E can masquerade as a server and try to respond with a valid message to the user. When the user U sends the login message $\langle X, T_u \rangle$ to the server, E can intercept the message and try to respond with the valid message. However, an adversary cannot successfully impersonate a valid user which is justified as follows:

E can try to responde with the old transmitted message $\langle Y, T_s \rangle$ to a user. However, the timestamp mechanism reveals the replay of message. Moreover, to replace T_s with current timestamp T_E, E has to compute $Y' = h(ID_U||sk'_{SU}||H)$ as $sk_{SU} = h(H \oplus r_u \oplus T_u \oplus T_S)$ includes timestamp. To compute sk_{SU}, H and r_u are needed.
E can try to responde with the message $\langle Y_E, T_E \rangle$, where $Y_E = h(ID_U||sk_{EU}||H)$ and $sk_{EU} = h(H \oplus r_E \oplus T_u \oplus T_S)$ for random value r_E and current timestamp T_E. To compute sk_{EU}, E needs H.
To retrieve H from v, the password is needed. Since the password is only known to the user, an adversary cannot get H.

This shows that the proposed scheme resists server impersonation attack.

3.2.10. Man-in-the middle attack

An adversary E may try to establish independent connections with license server and consumer. Since the user's message is encrypted with server's public key, an adversary cannot modify the user's message. Moreover, server's response message does not include any session value. This shows that the proposed scheme resists man-in-the middle attack.

3.2.11. Known key secrecy

An adversary cannot achieve or guess any secret from any compromised session key as the session key is the hashed output of user long-term key along with random value and timestamp, i.e., $sk = h(H \oplus r_u \oplus T_u \oplus T_s)$. Moreover, the secret key includes the timestamp which ensures a unique key for each session. These facts show that compromise of a particular session key does not result in compromise of the other session key.

3.2.12. Known session-specific temporary information attack

If the short term secret value r_u is compromised, then adversary cannot compute session key $sk = h(H \oplus r_u \oplus T_u)$ as to compute session key, user's long-term key H is needed along with the random value r_u where H is protected with the password.

3.2.13. Forward secrecy

If user's long-term key H is compromised, an adversary cannot achieve the established session key $sk = h(H \oplus r_u \oplus T_u \oplus T_s)$ as the session key includes a random value r_u, which is encrypted with the server's public key e, i.e., $X = (ID_U||r_u||R)^e \bmod N$. Therefore, an adversary cannot be achieved r_u using H.

3.2.14. Key freshness property

Each session key involves a random number and timestamp where random numbers and timestamps are different for each session. The uniqueness of these values guarantees the unique key for each session. The unique key construction for each session ensures the key freshness property.

3.2.15. Mutual authentication

Server verifies user's authenticity with the condition $R \stackrel{?}{=} h(ID_U||r_u||\ H||T_u)$ where to compute R, H and ID_U are needed. The user verifies authenticity of the server with the condition $Y \stackrel{?}{=} h(ID_U||sk||H)$, to compute Y, again H and ID_U are needed. Since, ID_U and H are secret, user and server can correctly verify the authenticity of each other.

4. Performance analysis

In this section, we show the efficiency analysis of proposed schemes with similar password based remote user authentication protocols based on smart card for the TMIS. Let the user identity ID, password PW, random variables, time stamp and output size of hash function is 128-bits while e, X, n all are of 1024-bits. Let T_h, T_E and T_X denote the time complexity of the hash function, exponential operation and XOR operation, respectively. It is well known that the time complexity of the XOR operation is negligible as compared to two other operations. So, we do not take T_X into account. In general, the time complexity associated with T_h, T_E and T_X can be more or less expressed as $T_E \gg T_h \gg T_X$ (Potlapally et al., 2006; Wong et al., 2001). Then, the extra communication and computation overheads are as follows:

In Lin's scheme, computation of W, CID, R, X is required in the login phase, and $X^d \bmod N, H, R, CID, \lambda, V, \lambda'$ and V' is required in the verification phase. So the computation overhead in the login phase is $3T_h + T_E$ and the verification phase is $7T_h + T_E$. The user and server transmit the messages $\langle X, R, T_1\rangle$ and $\langle V, \lambda\rangle$, therefore the communication overhead is $1536(= 4 \times 128 + 1024)$ bits. The smart card stores the values N, v, e and t, therefore, the memory required is $2304(= 2 \times 128 + 2 \times 1024)$.

In Xie et al.'s scheme, user's smart card computes $h(PW), A, C_1$ and AID in the login phase. Therefore, computation cost in the login phase is $2T_h + 2T_E$. In the verification phase, smart card computes K_{su}, sk_{su} and C'_u while server computes $AID^X(\bmod n), D_{sym_{(X)}}(RID), J, C_s, B, K_{us}, sk_{us}$ and C'_s. Therefore, the computation overhead in the verification phase is $6T_h + T_S + 4T_E$. The user transmits the message $\langle AID, T_u\rangle$ and $\langle C_2, T_s, B\rangle$, therefore the communication overhead is $2432(= 3 \times 128 + 2 \times 1024)$ bits. The smart card stores the values $\{ID, SC, N, L, n, e\}$, therefore, the memory required is $2660(= 4 \times 128 + 2 \times 1024)$ bits.

In Cao and Zhai's scheme, user's smart card computes $h(b||PW)$ and AID in the login phase. Therefore, computation cost in the login phase is $T_h + T_E$. In the verification phase, smart card computes K_{su}, C_s and C_u while the server computes $AID^X(\bmod n), J, K_s, C_s$ and C_u. Therefore, the computation overhead in the verification phase is $7T_h + T_E$. The user transmits the message $\langle AID\rangle, \langle r_s, C_s\rangle$ and C_u. Therefore the communication overhead is $1408(= 3 \times 128 + 1024)$ bits. The smart card stores the values $\{L, n, b\}$, therefore, the memory required is $1280(= 2 \times 128 + 1024)$ bits.

In the proposed scheme, computation of $h(PW_U||ID_U)$, W, B, R, X in the login phase and $X^d \bmod N, H$, R, sk_{SU}, Y, sk_{US} and Y in the verification phase. Therefore, the computation overhead in the login phase is $4T_h + T_E$ and the verification phase is $6T_h + T_E$. The user and server transmit the messages $\langle X, T_u\rangle$ and $\langle Y, T_s\rangle$, therefore the communication overhead is $1408(= 3 \times 128 + 1024)$ bits. The smart card stores the parameter N, v, e, A and B. Therefore, the required memory is $2432(= 3 \times 128 + 2 \times 1024)$. (see Table 3)

It can be easily seen from Table 1 that most of the authentication schemes for TMIS do not protect privacy. The dynamic ID based authentication schemes protect privacy, but do not resist denial of service attack (Lin, 2013; Xie et al., 2013). Chen et al.'s dynamic ID-based authentication scheme (Chen et al., 2012) and Cao and Zhai's dynamic ID-based authentication scheme (Cao and Zhai, 2013) efficiently resist denial of service attack, but Chen et al.'s scheme does not resist password and identity guessing attacks, while Cao and Zhai's scheme does not withstand known session specific temporary information attack. However, the proposed scheme protects privacy and resists guessing and denial of service attacks. Moreover, the proposed scheme resists known session specific temporary information attack and attains forward secrecy. The proposed scheme satisfies desirable security and it is comparable in terms of the communication and computational overheads with the relevant schemes, this makes the proposed scheme more appropriate for TMIS.

Table 3 Performance comparison between the proposed scheme and other relevant schemes.

Overhead/schemes	Chen et al.'s (2012)	Lin's (2013)	Cao and Zhai's (2013)	Xie et al.'s (2013)	Proposed scheme
l_1	384	2304 bits	1280	2660 bits	2432 bits
l_2	960	1536 bits	1408	2432 bits	1280 bits
l_3	$3T_h$	$3T_h + T_E$	$T_h + T_E$	$2T_h + 2T_E$	$4T_h + T_E$
l_4	$8T_h$	$7T_h + T_E$	$7T_h + T_E$	$6T_h + T_S + 4T_E$	$6T_h + T_E$
l_5	$11T_h$	$10T_h + 2T_E$	$8T_h + 2T_E$	$8T_h + T_S + 6T_E$	$10T_h + 2T_E$
l_6	2	2	3	2	2
S_1	√	√	√	√	√
S_2	×	√	√	√	√
S_3	×	√	√	√	√
S_4	×	√	√	×	√
S_5	√	√	√	√	√
S_6	×	√	√	√	√
S_7	√	√	×	×	√
S_8	√	√	√	√	√
S_9	√	×	√	×	√

l_1: storage overhead; l_2: communication overhead in login and authentication phases; l_3: computation overhead in login phase; l_4: computation overhead in verification phase; l_5: total computation overhead in login and authentication phases; l_6: number of messages exchanged; S_1: replay attack; S_2: user's impersonation attack; S_3: off-line password guessing attack; S_4: on-line password guessing attack; S_5: man-in-the middle attack; S_6: forward secrecy; S_7: known session specific temporary information attack; S_8: insider attack; S_9: denial of service attack.

5. Conclusion

We have discussed the failure of excising schemes for TMIS to present efficient login and password change phases in the literature. We have proposed an efficient and secure dynamic ID-based authentication scheme for TMIS. The proposed scheme maintains efficient login and password change phases where incorrect input can be quickly detected. Additionally, the scheme can efficiently resist guessing attacks and protect the user's privacy. Furthermore, the security analysis indicates that the proposed scheme satisfies all desirable security attributes. The performance analysis shows that the proposed scheme is comparable in terms of the communication and computational overheads with dynamic ID-based authentication schemes for TMIS.

References

Alfantookh, A.A., 2006. Dos attacks intelligent detection using neural networks. J. King Saud Univ. Comput. Inf. Sci. 18, 31–51.

Al-Muhtadi, J., 2007. An efficient overlay infrastructure for privacy-preserving communication on the internet. J. King Saud Univ. Comput. Inf. Sci. 19, 39–59.

Aloul, F., Zahidi, S., El-Hajj, W., 2009a. Multi factor authentication using mobile phones. Int. J. Math. Comput. Sci. 4 (2), 65–80.

Aloul, F., Zahidi, S., El-Hajj, W., 2009b. Two factor authentication using mobile phones. In: IEEE/ACS International Conference on Computer Systems and Applications, 2009. AICCSA 2009. IEEE, pp. 641–644.

Burrows, M., Abadi, M., Needham, R.M., 1989. A logic of authentication. Proc. R. Soc. London A. Math. Phys. Sci. 426 (1871), 233–271.

Cao, T., Zhai, J., 2013. Improved dynamic id-based authentication scheme for telecare medical information systems. J. Med. Syst. 37 (2), 1–7.

Chen, H.-M., Lo, J.-W., Yeh, C.-K., 2012. An efficient and secure dynamic id-based authentication scheme for telecare medical information systems. J. Med. Syst. 36 (6), 3907–3915.

He, D., Chen, J., Zhang, R., 2012. A more secure authentication scheme for telecare medicine information systems. J. Med. Syst. 36 (3), 1989–1995.

Jiang, Q., Ma, J., Ma, Z., Li, G., 2013. A privacy enhanced authentication scheme for telecare medical information systems. J. Med. Syst. 37 (1), 1–8.

Jiang, Q., Ma, J., Lu, X., Tian, Y., 2014. Robust chaotic map-based authentication and key agreement scheme with strong anonymity for telecare medicine information systems. J. Med. Syst. 38 (2), 1–8.

Lee, T.-F., Chang, I.-P., Lin, T.-H., Wang, C.-C., 2013. A secure and efficient password-based user authentication scheme using smart cards for the integrated epr information system. J. Med. Syst. 37 (3), 1–7.

Lin, H.-Y., 2013. On the security of a dynamic id-based authentication scheme for telecare medical information systems. J. Med. Syst. 37 (2), 1–5.

Mishra, D., 2015a. Understanding security failures of two authentication and key agreement schemes for telecare medicine information systems. J. Med. Syst. 39 (3), 1–8.

Mishra, D., 2015b. On the security flaws in id-based password authentication schemes for telecare medical information systems. J. Med. Syst. 39 (1), 1–16.

Mishra, D., Mukhopadhyay, S., 2014. A privacy enabling content distribution framework for digital rights management. Int. J. Trust Manag. Comput. Commun. 2 (1), 22–39.

Mishra, D., Mukhopadhyay, S., Kumari, S., Khan, M.K., Chaturvedi, A., 2014a. Security enhancement of a biometric based authentication scheme for telecare medicine information systems with nonce. J. Med. Syst. 38 (5), 1–11.

Mishra, D., Mukhopadhyay, S., Chaturvedi, A., Kumari, S., Khan, M.K., 2014b. Cryptanalysis and improvement of Yan et al.'s biometric-based authentication scheme for telecare medicine information systems. J. Med. Syst. 38 (6), 1–12.

Potlapally, N.R., Ravi, S., Raghunathan, A., Jha, N.K., 2006. A study of the energy consumption characteristics of cryptographic algorithms and security protocols. IEEE Trans. Mob. Comput. 5 (2), 128–143.

Syverson, P., Cervesato, I., 2001. The logic of authentication protocols. In: Foundations of Security Analysis and Design. Springer, pp. 63–137.

Wei, J., Hu, X., Liu, W., 2012. An improved authentication scheme for telecare medicine information systems. J. Med. Syst. 36 (6), 3597–3604.

Wong, D.S., Fuentes, H.H., Chan, A.H., 2001. The performance measurement of cryptographic primitives on palm devices. In: Proceedings 17th Annual Computer Security Applications Conference, 2001 (ACSAC 2001). IEEE, pp. 92–101.

Wu, F., Xu, L., 2013. Security analysis and improvement of a privacy authentication scheme for telecare medical information systems. J. Med. Syst. 37 (4), 1–9.

Wu, Z.-Y., Lee, Y.-C., Lai, F., Lee, H.-C., Chung, Y., 2012. A secure authentication scheme for telecare medicine information systems. J. Med. Syst. 36 (3), 1529–1535.

Xie, Q., Zhang, J., Dong, N., 2013. Robust anonymous authentication scheme for telecare medical information systems. J. Med. Syst. 37 (2), 1–8.

Xu, X., Zhu, P., Wen, Q., Jin, Z., Zhang, H., He, L., 2014. A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems. J. Med. Syst. 38 (1), 1–7.

Zhu, Z., 2012. An efficient authentication scheme for telecare medicine information systems. J. Med. Syst. 36 (6), 3833–3838.