Journal of King Saud University – Computer and Information Sciences (2015) 27, 211–221

King Saud University

Journal of King Saud University – Computer and Information Sciences

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

Cryptanalysis and improvement of a password-based user authentication scheme for the integrated EPR information system

SK Hafizul Islam [a,b,*], G.P. Biswas [b]

[a] Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani Campus, Rajasthan 333031, India
[b] Department of Computer Science and Engineering, Indian School of Mines, Dhanbad, Jharkhand 826004, India

Received 18 March 2013; revised 26 December 2013; accepted 13 March 2014
Available online 25 March 2015

KEYWORDS

EPR information system;
Two-factor user authentication;
Password;
Healthcare;
Smartcard;
Anonymity

Abstract Recently, Wu et al. proposed a password-based remote user authentication scheme for the integrated Electronic Patient Record (EPR) information system to achieve mutual authentication and session key agreement over the Internet. They claimed that the scheme resists various attacks and offers lower computation cost, data integrity, confidentiality and authenticity. However, we observed that the scheme cannot withstand lost smartcard/off-line password guessing, privileged-insider and known session-specific temporary information attacks, and lacks the requirements of lost smartcard revocation and users' anonymity. Besides, the password change phase is inconvenient to use because a user cannot change his password independently. Thus, we proposed a new password-based user authentication scheme for the integrated EPR information system that would be able to resist detected security flaws of Wu et al.'s scheme.

1. Introduction

The rapid growth of Information and Communication Technologies has the potential to support the transition from centralized computer systems to open networks (Chen et al., 2009). Thus, the historic paper-based medical information systems are now being replaced by the electronic media-based system known as e-medicine (Elberg, 2001). However, the e-medicine systems lack to gather patients' medical records scattered among different medical institutions. Since the patients often visited various medical institutions where they left their medical histories, so many times the doctors are facing problems to make correct diagnosis or clinical decision. Thus, an

* Corresponding author at: Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani Campus, Rajasthan 333031, India. Tel.: +91 8233348791/8797369160.
E-mail addresses: hafi786@gmail.com, hafizul.ism@gmail.com, hafizul@pilani.bits-pilani.ac.in (S.H. Islam).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jksuci.2014.03.018

integrated EPR information system is required for e-medicine to collect patients' paper-based information from different places, convert them to digital records and make them available so that any legitimate users (i.e., physicians, nurses, insurance companies, patients) can access over the Internet.

The EPR information system can be defined as electronic medium that can store complete or partial patients' records (Leiner et al., 2003) and now it becomes an essential medium for communication, research and monitoring medical information systems (Huang et al., 2011). It helps hospitals and medical institutions to back up patients' health information, and reduced the number of errors, loss of medical integration or failure of patients' medical histories. In addition, it offers enormous facility to the doctors to access patients' medical histories that not only assist to make correct clinical decisions, but also use to maintain and analyze patients' health. It also helps to access patients' information for management and resource planning of scientific research, or other services bound to be developed and integrated into e-medicine (Gritzalis et al., 2005). Besides, it can also provide patients' complete and correct medical problems along with other functions such as medical alerts or reminders, clinical decision support, and links to their medical supporting groups.

The EPR information system requires a mutual authentication mechanism that allows legitimate users to access patients' medical information stored on a remote server. However, security and privacy are two major issues, since the communication channel is often sniffed by benign adversary who can intercept, modify and delete the messages. To cope these problems, two-factor user authentication (TF-UA) with key agreement (Wu et al., 2010, 2011a,b; Debiao et al., 2012; Wei et al., 2012) is generally used in which password- and smartcard-based TF-UA mechanism is popular. Furthermore, anonymous TF-UA (Liao and Wang, 2009; Wang et al., 2009, 2011) is the most suitable mechanism that mutually authenticates both user and server without disclosing the real identity to others (Islam and Biswas, 2011; Khan et al., 2011).

Recently, Wu et al. (2010) proposed a smartcard-based password authentication scheme for the Telecare Medicine Information System (TIMS), which is vulnerable to the impersonation and insider attacks (Khan and Alghathbar, 2010) as proven by (Debiao et al., 2012). In (Debiao et al., 2012), the authors presented a new TF-UA scheme for TIMS to remove the loopholes of (Wu et al., 2010). However, Wei et al. (2012) shows that both the schemes (Wu et al., 2010; Debiao et al., 2012) fail to protect off-line password guessing attack, i.e., an outsider can guess users' password if he extracts the secret information stored in the smartcard by monitoring timing information, power consumption and reverse engineering techniques (Kocher et al., 1999; Messerges et al., 2002). Then Wei et al. proposed an improved TF-UA scheme. Recently, Wu et al. (2012) proposed a TF-UA scheme for the integrated EPR information system, however we identified that the scheme is vulnerable to lost smartcard/off-line password guessing (Islam and Biswas, 2013a), privileged-insider (Khan and Alghathbar, 2010) and known session-specific temporary information (Islam and Biswas, 2012a) attacks. Also the scheme does not provide a provision for lost smartcard revocation (Fan et al., 2005; Khan et al., 2011) and users' anonymity (Liao and Wang, 2009; Islam and Biswas, 2011). Furthermore, the password change phase is inconvenient to use since the user cannot change his password without server's assistance. In this paper, we proposed an enhanced TF-UA scheme for the integrated EPR information system with enhanced security compared to the existing schemes.

The rest of the paper is divided into following sections. We described Wu et al.'s TF-UA system in Section 2 and its drawbacks are given in Section 3. In Section 4, we proposed a TF-UA scheme and analyzed its security and performance in Section 5. Finally, Section 6 draws some concluding remarks.

2. Review of Wu et al.'s user authentication scheme for integrated EPR information system

In this section, we briefly reviewed Wu et al.'s user authentication scheme (Wu et al., 2012) and the notations are listed in Table 1. The scheme is divided into four phases: registration phase, login phase, verification phase and password change phase.

2.1. Registration phase

In this phase, user A registers to S to obtain a medical smartcard. For this purpose, A sends a registration request to S and then S performs the following operations:

(R-1). A chooses an identity ID and a password pw, and then submits (ID, pw) to S through a secure channel.
(R-2). S first verifies ID and computes $v = h(K \oplus ID)$, where the secret number K is chosen by S.
(R-3). S chooses a N and computes $[H = v \cdot pw + N, s = h(pw||K)]$, where the secret H is different for every user.
(R-4). S issues a smartcard with the parameters $[h(\cdot), N, s]$ and returns it to A through a secure channel.

2.2. Login phase

In this phase, A inserts his smartcard into a card reader and keys his (ID, pw). Then the smartcard performs the following:

(L-1). Smartcard chooses a random number r_1 and computes (C_1, C_2), where $C_1 = h(s||r_1)$ and $C_2 = r_1 \cdot pw$.
(L-2). Smartcard retrieves N and sends $\{ID, N, C_1, C_2\}$ to S through open channel.

2.3. Verification phase

(V-1). S verifies ID of $\{ID, N, C_1, C_2\}$. If it is valid, S proceeds to the next step, otherwise rejects A's request.

Table 1 Notations used in Wu et al.'s scheme.

Notations	Meaning
A	The medical service requester (user)
pw	The password of user A
ID	The identity of user A
S	The integrated EPR information system (server)
$h(\cdot)$	One-way and secure cryptographic hash function
$\oplus$	Bit-wise XOR operation
$\|\|$	Concatenation operator

(V-2). S uses his own secret values K and H, and computes $v = h(K \oplus ID)$ and $pw = (H - N) \cdot v^{-1}$.
(V-3). S calculates $r_1' = pw^{-1} \cdot C_2$ and the secret value $s' = h(pw||K)$.
(V-4). S checks whether $h(s'||r_1') = ?C_1$. If not, S sends an error message to A, otherwise go to the next step.
(V-5). S chooses a random number r_2, computes $a = r_2 \oplus h(s')$, $b = h(pw||r_2||r_1')$ and sends (a, b) to A through an open channel.
(V-6). Upon receiving (a, b), A computes $r_2' = a \oplus h(s)$ and verifies whether b is equal to $h(pw||r_2'||r_1)$. If they are equal, A confirms that S is valid and sends a message $c = h(pw||r_1||r_2')$ to S.
(V-7). S compares c with $h(pw||r_1'||r_2)$ to check whether both of them are same or not. If so, A is authenticated by S. After the mutual authentication, both A and S accept $sk = h(r_1'||r_2) = h(r_1||r_2') = h(r_1||r_2)$ as a session key.

2.4. Password change phase

(P-1). A sends his old (ID, pw) along with a new password pw_{new} to S through a secure channel.
(P-2). S chooses another appropriate number N^* to calculate $H^* = v \bullet pw_{new} + N^*$. Then S computes $s^* = h(pw_{new}||K)$, and sends $[s^*, N^*]$ to A through a secure channel.

3. Weaknesses of Wu et al.'s user authentication scheme

Wu et al.'s scheme is analyzed, and some weaknesses are investigated and explored in this section.

3.1. Lost smartcard attack/off-line password guessing attack

Wu et al.'s scheme is a password- and smartcard-based TF-UA scheme in which the smartcard contains secret information $[h(\cdot), N, s]$ about A, which at a later time is used to authenticate A. The smartcard-based TF-UA scheme faces the threat of smartcard security attack while some sensitive information is stored in the card. The authentication system will be compromised if an attacker extracts the secrets from the smartcard, and thus some additional mechanism should be taken by the designer to protect this kind of threat. It is pointed out by Kocher et al. (1999) and Messerges et al. (2002) that all the existent smartcard-based schemes are susceptible to lost/stolen smartcard attack through differential power analysis, because the confidential information stored in the card could be extracted by physically monitoring its timing information, power consumption and reverse engineering techniques; since once a card has been lost, all secrets in it may be compromised. Accordingly Wu et al.'s scheme is vulnerable to this attack (Vaidya et al., 2010; Khan et al., 2011) and its description is given below:

(1) Suppose an adversary E extracts $[h(\cdot), N, s]$ from A's lost smartcard.
(2) E collects a valid login message $\{ID, N, C_1, C_2\}$ from the previous session, where $C_1 = h(s||r_1)$ and $C_2 = r_1 \cdot pw$. It is to be noted that $r_1 = C_2/pw$ and thus, we can write $C_1 = h(s||C_2/pw)$.
(3) Now, E guesses a password pw^*, computes $C_1^* = h(s||C_2/pw^*)$ and checks whether $C_1^* = C_1$ holds. If it is, then $pw^* = pw$, otherwise the steps 2 and 3 are repeated until the correct pw is found.

E can easily find A's password pw just by testing all possible passwords from the search space $|D|$, where $|D|$ is the set of all possible passwords and $|\bullet|$ represents the cardinality of D. This kind of off-line password guessing attack is possible within polynomial-time bound, because user generally chooses a weak password (low-intensity) for easy memorization and $|D|$ is not large enough.

3.2. Absence of lost smartcard revocation phase

If a smartcard is lost/stolen and its secret values are known to an adversary with the help of the techniques proposed in (Kocher et al., 1999; Messerges et al., 2002), then he can guess users' password by applying off-line password guessing attack (Vaidya et al., 2010; Khan et al., 2011) on the extracted information. Thus, the revocation of lost/stolen smartcard is necessary in order to offer strong security to the end users (Fan et al., 2005). Otherwise the adversary may impersonate the legal user to login to the server using the lost/stolen smartcard and old password if the server is unable to distinguish the new smartcard from the lost card (Khan et al., 2011). However, Wu et al.'s scheme lacks such a lost smartcard revocation phase.

3.3. Privileged-insider attack

Wu et al.'s scheme is vulnerable to the privileged-insider attack. In the registration phase, A sends his (ID, PW) in plain text form to S to get a valid smartcard. A privileged-insider E of S can easily steal (ID, pw) and can perform the malicious activity in the following way. If A is registered by the same password pw to other remote servers outsides S for their convenience of remembering a long password and ease-of-use, then E can impersonate A by accessing other servers by using the same pw if all the servers adopt the same authentication procedure (Khan and Alghathbar, 2010; Debiao et al., 2012).

3.4. Inconvenient password change phase

Wu et al.'s password change phase is not user-friendly. In password change, A sends his old (ID, pw) along with a new password pw^* to S through a secure channel. Then S chooses a number N^*, calculates $H^* = v \cdot pw^* + N^*$ and $s^* = h(pw^*||K)$ and sends $[s^*, N^*]$ to A through a secure channel. Thus, A cannot change his password frequently since every time he has to use the secure channel, which is very difficult to achieve in practice. In addition, the password change phase is different from the traditional smartcard-based schemes (Vaidya et al., 2010; Khan and Alghathbar, 2010), in which password can be changed directly by the user without remote server's assistance. So the frequent password change will put additional burden on the system.

3.5. Known session-specific temporary information attack

According to (Canetti and Krawczyk, 2001; Cheng et al., 2005; Swanson, 2008), the known session-specific temporary

information attack means that the exposer of ephemeral secrets of a session may harm the secrecy of session key. It is pointed out by (Mandt and Tan, 2008; Hou et al., 2010) that this attack is quite practical in some situations since (1) user and server must trust the internal/external source of random number generator that may be controlled by an adversary, and (2) the random numbers are generally stored in insecure memory device whereas long-term secrets are protected carefully. If the random numbers are not erased properly after the protocol execution, an adversary may hijack users' computer and get the random numbers. Thus, the authentication scheme must have the additional ability that could resist this attack. However, Wu et al.'s scheme is insecure against this attack where A and S generate the session key $sk = h(r_1||r_2)$ and it can be compromised if r_1 and r_2 are known to an adversary E. Moreover, this disclosure also leads to compromise A's password pw from the eavesdropped message $\{ID, N, C_1 = h(s||r_1), C_2 = r_1 \cdot pw\}$ as $pw = C_2/r_1$. Thus, Wu et al.'s scheme needs some countermeasures to protect these problems.

3.6. Lack of users' anonymity

In practice, one of the fundamental requirements for secure communication over an insecure network is users' anonymity (Wong et al., 2006; Wang et al., 2009), which makes it very difficult to recognize the original user from the login message by an outsider. That is, to preserve secrecy, a user instead of his static identity, sends a dynamic identity which is calculated by binding some secret information with the static identity, otherwise a login message with a static identity reveals some personal information about the user. An outsider may intercept the user's login message and try to manipulate with other parameters to forge login identity known as identity-theft attack (Liao and Wang, 2009). Wu et al. scheme does not achieve users' anonymity. During the authentication phase of Wu et al.'s scheme, A sends $\{ID, N, C_1, C_2\}$ to S over a public network, which contains the static login identity ID from which E can easily recognize that the transaction is performed by A (Khan and Alghathbar, 2010). Thus, Wu et al.'s scheme does not provide users' anonymity.

3.7. Other drawbacks of Wu et al.'s authentication system

In addition to the above, Wu et al.'s scheme has some other drawbacks as given below.

(1) For each user two secrets K and H are kept secret by S, where K is identical for all users whereas H varies from user to user. Thus, S has to keep $(n + 1)$ secret keys i.e., a single K and n different H for n users. In practice, it is possible to achieve mutual authentication between the server and user by using only one secret key (Wang et al., 2009; Islam and Biswas, 2011). Thus, more than one secret puts unnecessary burden on S without increasing security of the system (Khan and Alghathbar, 2010; Vaidya et al., 2010).

(2) In the login phase, smartcard computes $\{ID, N, C_1, C_2\}$ without checking the validity of (ID, pw) that leads the system to suffer from *clogging attack*, a type of denial of service (DoS) attack in which E attempts to deny service by overwhelming the resources of S by replaying a large volume of fake authentication messages. For instance, assume that E steals A's smartcard and computes some fake login messages of type $\{ID, N, C_1^*, C_2^*\}$ with a false pw^* along with real identity ID. If E submits a large number of such fake messages, S will be busy to process these messages and meanwhile other legitimate users get rejected while they are trying to authenticate themselves to S.

4. Proposed scheme for the integrated EPR information system

In this section, we proposed a password and smartcard-based TF-UA scheme for the integrated EPR medical information system using Chen et al.'s scheme (2008) and Schnorr's signature scheme (1990). The notations used in the scheme are listed in Table 2. Our scheme is composed of the following phases.

4.1. Initialization phase

In this phase, for given a security parameter $k \in Z^+$, S initializes the system's parameter as follows:

(I-1) S chooses two large primes p and q such that $p = 2q + 1$ and a generator g of Z_p^*.

(I-2) S chooses its private key $x \in Z_p^*$ and then computes the public key $y = g^x \bmod p$.

(I-3) S selects a one-way secure cryptographic hash function $H : \{0,1\}^* \rightarrow \{0,1\}^k$

(I-4) Finally, S publishes the system's parameter $\Omega = \{p, g, H, y\}$, while the private key x is kept secret.

4.2. Registration phase

(R-1). A chooses an identity-password pair (ID_a, PW_a) and a $d_a \in_R Z_p^*$, computes $V_a = H(ID_a||PW_a||d_a)$, and sends (ID_a, V_a) to S over a secure channel.

(R-2). S checks whether ID_a already exists in the database. If so, S asks A for a fresh identity. Then S selects a $d_s \in_R Z_p^*$, computes $D_s = g^{d_s} \bmod p$ and $\sigma_s = d_s - xe_s \bmod p$, where $e_s = H(ID_a||D_s||SN)$.

(R-3). S computes $V_s = H(ID_a||d_s||SN)$, $V_{as} = H(V_a) \oplus e_s$, inserts $[ID_a, \sigma_s, e_s, V_s, V_{as}, y, H(\cdot)]$ into the smartcard and

Table 2 Notations used in the proposed scheme.

Notations	Meaning
PW_a	Password of the user A
ID_a	Identity of A
k	Security parameter
p, q	Two large primes p and q such that $p = 2q + 1$
Z_p^*	Multiplicative group of prime order p
g	Generator of the group Z_p^*
x, y	Private and public key of S, where $y = g^x \bmod p$
SN	Identity/serial number of the smartcard
$H(\cdot)$	One-way and secure cryptographic hash function, where H: $\{0, 1\}^* \rightarrow \{0, 1\}^k$
T_a/T_s	Timestamp chosen by A/S
SK	Session key
E	Adversary/privileged-insider

returns it to A through a secure channel. Then S stores (ID_a, SN) in the database.

(R-4). Now A inserts d_a into the smartcard and replaces V_s by H_a, where $H_a = V_s \oplus V_a$. Finally, the smartcard contains the information $[ID_a, \sigma_s, e_s, H_a, V_{as}, y, d_a, H(\cdot)]$.

4.3. Login phase

(L-1). A inserts his smartcard into a card reader and keys (ID_a, PW_a). Smartcard then checks whether the supplied ID_a is matched with the stored identity. If not, the smartcard asks A for a valid identity-password pair, otherwise computes $V_a = H(ID_a||PW_a||d_a)$ and $e'_s = V_{as} \oplus H(V_a)$, and then checks whether $e'_s = e_s$ holds. If so, the smartcard chooses a $r_a \in_R Z_q^*$, computes $R_a = g^{r_a} \bmod p$ and $V_s = H_a \oplus V_a$.

(L-2). Smartcard chooses a current timestamp T_a, computes $DI_a = ID_a \oplus H(T_a||y^{r_a})$ and $C_a = H(ID_a||R_a||\sigma_s||e_s||T_a||V_s)$, and then sends $M_1 = \{DI_a, C_a, R_a, T_a, \sigma_s, e_s\}$ to S.

4.4. Mutual authentication with session key agreement phase

(V-1). S checks whether $T'_a - T_a \leqslant \Delta T_a$ holds. If not, S rejects A's login request, otherwise goes to next step.

(V-2). S computes $ID_a = DI_a \oplus H(T_a||R_a^x)$ and rejects A's login request if the computed identity is invalid.

(V-3). S obtains SN from the database, computes $d_s = \sigma_s + xe_s \bmod p$, $V_s = H(ID_a||d_s||SN)$ and $C'_a = H(ID_a||R_a||\sigma_s||e_s||T_a||V_s)$, and verifies whether $C'_a = C_a$ is valid. If the result is negative, S rejects the login request, otherwise authenticates A.

(V-4). S chooses a $r_s \in_R Z_q^*$, a current timestamp T_s, computes $R_s = g^{r_s} \bmod p$, $K = (R_a)^{r_s} \bmod p = g^{r_a r_s}$ and the session key $SK = H(ID_a||T_a||T_s||R_a||R_s||K||V_s)$. S then sends $M_2 = \{C_S, R_S, T_s\}$ to A through a public channel, where $C_s = H(ID_a||R_a||R_s||T_s||V_s||SK)$.

(V-5). Upon receiving $M_2 = \{C_s, R_s, T_s\}$, A checks whether $T'_s - T_s \leqslant \Delta T_s$ holds. If it fails, A rejects $M_2 = \{C_s, R_s, T_s\}$, otherwise proceeds to the next step.

(V-6). A computes $K = (R_s)^{r_a} \bmod p = g^{r_a r_s}$, $SK = H(ID_a||T_a||T_s||R_a||R_s||K||V_s)$ and $C'_s = H(ID_a||R_a||R_s||T_s||V_s||SK)$. If $C'_s = C_s$ holds, A authenticates S and accepts the session key SK.

4.5. Password change phase

(P-1). A inserts the smartcard into the card reader and keys the old identity-password pair (ID_a, PW_a). Smartcard checks whether the supplied identity ID_a is valid or not by comparing it with the stored identity in the card. If not, smartcard rejects the request, otherwise computes $V_a = H(ID_a||PW_a||d_a)$, $e'_s = V_{as} \oplus H(V_a)$ and verifies $e'_s = e_s$. If it is, smartcard asks A for a new password.

(P-2). A keys a new password PW_{anew} and then the smartcard computes $V_{anew} = H(ID_a||PW_{anew}||d_a)$, $V_{asnew} = H(V_{anew}) \oplus e_s$ and $H_{anew} = H_a \oplus V_a \oplus V_{anew}$. Finally, smartcard's memory is updated by replacing $[ID_a, \sigma_s, e_s, H_a, V_{as}, y, d_a, H(\cdot)]$ with $[ID_a, \sigma_s, e_s, H_{anew}, V_{asnew}, y, d_a, H(\cdot)]$.

4.6. Lost smartcard revocation phase

To revoke a lost/stolen smartcard, our scheme performs the following operations:

(S-1). A picks a $d'_a \in_R Z_p^*$, computes $V'_a = H(ID_a||PW_a||d'_a)$ and sends (ID_a, V'_a) to S over a secure channel.

(S-2). S checks A's credentials, e.g., date of birth, national ID card number, or some other values from which A can be uniquely identified. Afterward, S reads the serial number SN' from the new card, selects a $d'_s \in_R Z_p^*$, computes $D'_s = g^{d'_s} \bmod p$ and $\sigma'_s = d'_s - xe'_s \bmod p$, where $e'_s = H(ID_a||D'_s||SN')$.

(S-3). S also computes $V'_s = H(ID_a||d'_s||SN')$ and $V'_{as} = H(V'_a) \oplus e'_s$. S inserts $[ID_a, \sigma'_s, e'_s, V'_s, V'_{as}, y, H(\cdot)]$ into the new card, returns it to A over a secure channel and updates (ID_a, SN) with (ID_a, SN') to the database.

(S-4). Now, A inserts d'_a into the new card and replaces V'_s by H'_a, where $H'_a = V'_s \oplus V'_a$. Finally, the new smartcard contains the information $[ID_a, \sigma'_s, e'_s, H'_a, V'_{as}, y, d'_a, H(\cdot)]$.

In case of revocation of lost/stolen smartcard, there exists another serious problem. If the smartcard and password both are lost, then the user is strongly recommended to re-register with a new password to the server to get a new smartcard even if the system is able to resist the off-line password guessing attack. Otherwise, an adversary can masquerade the legitimate user using the lost smartcard and password.

5. Security and efficiency analysis of the proposed scheme

This section analyzes the security aspects of our scheme and also compares with the previous schemes.

5.1. Informal security analysis

In this section, we will provide an informal security analysis of our scheme that satisfies most of the security requirements as discussed below:

5.1.1. Replay and parallel session attack

This attack may occur frequently from an active adversary who tries to impersonate a legitimate user/server by replaying some eavesdropped messages. Suppose E collects A's login message $M_1 = \{DI_a, C_a, R_a, T_a, \sigma_s, e_s\}$ from the previous session and replays it to S in the current session. However, S rejects E as $T'_a - T_a \leqslant \Delta T_a$ is invalid. Furthermore, E may send a modified message $M''_1 = \{DI_a, C_a, R_a, T''_a, \sigma_s, e_s\}$ to S, where T''_a is the current timestamp. In this case, E also gets rejected since $C''_a \neq C_a$. Also, E cannot impersonate S by replaying an old message $M_2 = \{C_s, R_s, T_s\}$ and thus, our scheme is secured from this attack. Besides, our scheme also resists parallel session attack in which an adversary tries to impersonate a legal user without knowing the correct password. In this

attack, E attempts to generate a valid authentication message from the previous messages. Suppose E collects $M_1 = \{DI_a, C_a, R_a, T_a, \sigma_s, e_s\}$ and $M_2 = \{C_s, R_s, T_s\}$, however, he cannot generate any fabricated valid login and authentication messages from $\{M_1, M_2\}$ without the secret key and the secret values stored on the smartcard. Furthermore, E cannot impersonate A just by replaying the eavesdropped messages $\{M_1, M_2\}$ due to the inclusion of time stamps T_a and T_s in $\{M_1, M_2\}$.

5.1.2. Off-line/On-line password guessing attack

In general, a user chooses a weak password for easy memorization and therefore, the password guessing attack (Liao and Wang, 2009; Vaidya et al., 2010) may occur from an active adversary if an efficient scheme is not followed. Suppose E collects $[ID_a, \sigma_s, e_s, H_a, V_{as}, y, d_a, H(\cdot)]$ from the lost/stolen smartcard using differential power analysis (Kocher et al., 1999; Messerges et al., 2002) and tries to guess the correct password by applying some off-line mechanism on $H_a = V_s \oplus V_a$, $V_s = H(ID_a||d_s||SN)$ and $V_a = H(ID_a||PW_a||d_a)$. To obtain V_a from H_a, and PW_a from V_a, E must learn the random number d_s chosen by S. However, the probability of guessing it and thus the password is 2^{-k} , where k is the security parameter. So the off-line password guessing attack is hard. On the other hand, our scheme also protects on-line password guessing attack in which E guesses a password of A and generates a fabricated login message and sends it to S. E repeats this process until to get login to S. If this happens, it indicates that E successfully masquerade A. Now E guesses a password PW_a^*, chooses $H_a^*, \sigma_s^*, e_s^*, d_a^*, r_a^* \in_R Z_q^*$, a timestamp T_a^*, computes $R_a^* = g^{r_a^*} \bmod p$, $DI_a^* = ID_a \oplus H(T_a^*||y^{r_a^*})$, $V_s^* = H_a^* \oplus H(ID_a||PW_a^*||d_a^*)$, $C_a^* = H(ID_a||R_a^*||\sigma_s^*||e_s^*||T_a^*||V_s^*)$ and sends $M_1^* = \{DI_a^*, C_a^*, R_a^*, T_a^*, \sigma_s^*, e_s^*\}$ to S. Then S computes $ID_a = DI_a^* \oplus H(T_a^*||(R_a^*)^x)$, $d_s'' = \sigma_s^* + xe_s^*$, $V_s'' = H(ID_a||d_s''||SN)$ and $C_a'' = H(ID_a||R_a^*||\sigma_s^*||e_s^*||T_a^*||V_s'')$, and observes that $C_a'' \neq C_a^*$ since $V_s'' \neq V_s^*$. Therefore, S rejects authentication request made by E.

5.1.3. Privileged-insider attack

In real-life application, a user may access different servers by using the same identity and password for his convenience. However, if a privileged-insider of S learns the password PW_a of A, he may of course impersonate A by using the stolen password to get access to all the servers, where A is registered as a legitimate user. However, our scheme can make this kind of attack ineffectual, since A is registered to S by sending (ID_a, V_a) instead of (ID_a, PW_a), where d_a in $V_a = H(ID_a||PW_a||d_a)$ is unknown to the insider of S, so he cannot obtainPW_a just by performing off-line guessing attack on V_a.

5.1.4. Impersonation attack

To make this attack successful, E tries to authenticate himself maliciously as A to S (or as S to A). However, this attack is infeasible in our scheme since E cannot generate A's login message $M_1 = \{DI_a, C_a, R_a, T_a, \sigma_s, e_s\}$ without smartcard and password PW_a. Because E cannot compute $V_s = H_a \oplus H(ID_a||PW_a||d_a)$ and $C_a = H(ID_a||R_a||\sigma_s||e_s||T_a||V_s)$ as well. In other way, server's impersonation attack is also infeasible here since E cannot generate $M_2 = \{C_s, R_s, T_s\}$ without x, where $d_s = \sigma_s + xe_s$ and $V_s = H(ID_a||d_s||SN)$. Also, E cannot compute x from the public key $y = g^x \bmod p$ due to DLP and thus, this attack is hard in our scheme.

5.1.5. User's anonymity problem

In login phase, user A transmits a dynamic identity $DI_a = ID_a \oplus H(T_a||y^{r_a})$, which differs session to session due to T_a and r_a. The random number r_a is unknown to E so he cannot extract ID_a from DI_a and also it cannot be guessed within polynomial-time. Thus, users' anonymity is achieved in our scheme.

5.1.6. Mutual authentication and session key agreement

The login and mutual authentication with session key agreement phases are necessary in an authentication system to provide the data security and privacy of the user who wish to communicate with a remote server over insecure channel. Our scheme supports secure mutual authentication and session key generation.

5.1.7. Protection of data integrity

The protection and integrity of data during transmission over insecure network is achieved in our scheme in two ways. Firstly, the integrity of login and authentication of messages is done safely at the server- and user-side using $C_a' = C_a$ and $C_s' = C_s$. Secondly, during transmission the integrity, confidentiality and security of data are achieved using the session key SK. After mutual authentication and session key agreement, the sensitive messages are encrypted with the session key and then transmitted over an open channel so the eavesdropper cannot infringe the privacy of the message.

5.1.8. Session key perfect forward secrecy

Our scheme satisfies the session key perfect forward secrecy (Blake-Wilson et al., 1997), i.e., even if the secret key x is disclosed, E cannot impersonate A. Because E cannot generate a valid session key $SK = H(ID_a||T_a||T_s||R_a||R_s||K||V_s)$ without $K = g^{r_a r_s}$ and $V_s = H(ID_a||d_s||SN)$. Thus, our scheme provides session key perfect forward secrecy.

5.1.9. Known session-specific temporary information attack

The proposed scheme protects the known session-specific temporary information attack (Islam and Biswas, 2011, 2013a). In our scheme, S and A compute the session key $SK = H(ID_a||T_a||T_s||R_a||R_s||K||V_s)$, where $K = g^{r_a r_s}$ and $V_s = H(ID_a||d_s||SN)$. If the session ephemeral secrets r_a and r_s are compromised, however SK is still secured, because $V_s = H(ID_a||d_s||SN)$ is unknown to E.

5.1.10. Known-key attack

The known-key attack means that E cannot compute any of the future/previous session keys even if the current session key is compromised (Blake-Wilson et al., 1997). In our scheme, a fresh session key SK is generated in each session by using random numbers r_a and r_s. The freshness of SK depends on r_a and r_s. Suppose a session key SK of the current session is compromised to E, however due to the one-way property of the hash function, E will not be able to derive any secrets. Thus, other session keys cannot be generated from the knowledge of the leaked session key.

5.2. Formal security analysis

According to (Chatterjee et al., 2014; Das and Bruhadeshwar, 2013), in this section, we discussed the formal analysis about the security of the proposed scheme.

Definition 1 (*Negligible function*). A function $\varepsilon(k)$ is said to be negligible, if for every $c > 0$, there exists k_0 such that $\varepsilon(k) \leqslant k^{-c}$ for every $k \geqslant k_0$.

Definition 2 (*Formal definition of one-way cryptographic hash function*). A collision resistant one-way cryptographic hash function $H(\bullet) : X \to Y$, where $X = \{0,1\}^*$ and $Y = \{0,1\}^k$, is a deterministic algorithm that takes $x \in \{0,1\}^*$ as input and outputs $y = H(x) \in \{0,1\}^k$. If $Adv_E^{Hash}(t_1)$ denotes the advantage in finding a collision by a probabilistic polynomial-time bound adversary E, we defined

$$Adv_E^{Hash}(t_1) = \Pr[E_R(x_1, x_2) : x_1 \neq x_2 \text{ and } H(x_1) = H(x_2)],$$

where $\Pr[X]$ denotes the probability of a random event X, and $E_R(x_1, x_2)$ denotes the pair (x_1, x_2) is selected randomly by E. The probability of success in finding a collision in $H(\cdot)$ is computed over the random choices made by E with the execution time t_1. The hash function $H(\cdot)$ is then called collision resistant, if $Adv_E^{Hash}(t_1) \leqslant \varepsilon_1$, for any sufficiently small $\varepsilon_1 > 0$.

Definition 3 (*Formal definition of discrete logarithm problem*). Let p and q are two large prime numbers such that $p = 2q + 1$ and g be a generator of a multiplicative cyclic group Z_p^* of order p. The discrete logarithm problem (DLP) states that for given (g, g^a), it is computationally hard by any polynomial-time bounded algorithm E for finding a, where $a \in Z_p^*$ is unknown to him. Formally, if $Adv_E^{DLP}(t_2)$ denotes an adversary A's advantage in finding a, we have $Adv_E^{DLP}(t_2) = \Pr[E(g, g^a) = a : a \in Z_p^*]$. The probability of success of finding a from (g, g^a) in $Adv_E^{DLP}(t_2)$ is computed over the random choices made by E with the execution time t_2. The DLP is computationally infeasible, if $Adv_E^{DLP}(t_2) \leqslant \varepsilon_2$, for any sufficiently small $\varepsilon_2 > 0$.

We then define the following random oracles for the formal security analysis:

- *Reveal*1: This random oracle will unconditionally output the input x from the corresponding hash value $y = h(x)$.
- *Reveal*2: This random oracle will unconditionally output a from the pair (g, g^a).

Theorem 1. Suppose that the hash function closely behaves like a random oracle, then the proposed scheme is provably secure against a probabilistic polynomial-time bounded adversary for deriving the session key established between the user and the server.

Proof. Assume that E is a probabilistic polynomial-time bounded adversary, who runs the experiment $Exp1_E^{Hash}$ in order to break the security of the session key SK of the proposed scheme. We defined the success probability for the experiment $Exp1_E^{Hash}$ as $Succ1 = 2\Pr[Exp1_E^{Hash} = 1] - 1$. The advantage of $Exp1_E^{Hash}$ is defined as $Adv1(et_1, q_{R1}) = Max_E\{Succ1\}$, where the maximum is taken over all E with the execution time et_1 and the number of queries q_{R1} made to the oracle *Reveal*1. We can say that the proposed scheme is provably secure against E for deriving the session key SK between the user A and the server S, if $Adv1(et_1, q_{R1}) \leqslant \varepsilon_3$, for any sufficiently small $\varepsilon_3 > 0$. Based on the experiment given below (algorithm 1), E can derive the session key SK from the transmitted messages between A and S, if he/she has the ability to invert the one-way hash function $H(\bullet)$. From the Definition 2, we have $Adv1_E^{Hash}(t_1) \leqslant \varepsilon_1$ for any sufficiently small $\varepsilon_1 > 0$ and thus the advantage $Adv1(et_1, q_{R1})$ is negligible, since it depends on $Adv1_E^{Hash}(t_1)$. Therefore, E will get success for deriving the session key SK with negligible probability and as a result, the proposed scheme is provably secure against E. □

Algorithm 1: $Exp1_E^{Hash}$

1: Intercept the message $M_2 = \{C_S, R_S, T_s\}$ during authentication phase sent to the user A by the server S, where $C_s = H(ID_a||R_a||R_s||T_s||V_s||SK)$
2: Call *Reveal1* oracle on input C_s to retrieve ID_a, R_a, R_s, T_s, V_s and SK as $(ID_a^*||R_a^*||R_s^*||T_s^*||V_s^*||SK^*) \leftarrow Reveal1(C_s)$
3: Intercept the message $M_1 = \{DI_a, C_a, R_a, T_a, \sigma_s, e_s\}$ during the login phase sent from A to S, where $C_a = H(ID_a||R_a||\sigma_s||e_s||T_a||V_s)$
4: Call the oracle *Reveal1* on input C_a to retrieve ID_a, R_a, σ_s, e_s, T_a and V_s as $(ID_a^{**}||R_a^{**}||\sigma_s^{**}||e_s^{**}||T_a^{**}||V_s^{**}) \leftarrow Reveal1(C_a)$
5: If $(ID_a^{**} = ID_a^*)$ and $(R_a^{**} = R_a^*)$ and $(R_s^{**} = R_s^*)$ and $(V_s^{**} = V_s^*)$ then
6: Accept SK^* as the correct session key SK shared between A and S
7: Return 1 (Success)
8: Else
9: Return 0 (Failure)
10: End If

Theorem 2. Assume that hash function closely behaves like a random oracle and the hardness of DLP, the proposed scheme is provably secure against a probabilistic polynomial-time bounded adversary for deriving the password of the user and the secret key of the server, even if the adversary extracts all the secret information from the lost/stolen smartcard.

Proof. Assume that E runs the experiment $Exp2_{DLP,E}^{Hash}$, which is described below (algorithm 2), in order to obtain the password PW_a of A and the secret key x of S from the information stored in A's smartcard. We defined the success probability for the experiment $Exp2_{DLP,E}^{Hash}$ as $Succ2 = 2\Pr[Exp2_{DLP,E}^{Hash} = 1] - 1$. The advantage of $Exp2_{DLP,E}^{Hash}$ is defined as $Adv2(et_2, q_{R1}, e_{R2}) = Max_E\{Succ2\}$, where the maximum is taken over all E with the execution time et_2 and the number of queries q_{R1} and q_{R2} made to the oracles *Reveal*1 and *Reveal*2. We can say that the proposed scheme is provably secure against E for deriving the password PW_a of A and the secret key x of S, if $Adv2(et_2, q_{R1}, e_{R2}) \leqslant \varepsilon_4$, for any sufficiently small $\varepsilon_4 > 0$. Based on the experiment $Exp2_{DLP,E}^{Hash}$, E can extract the

Table 3 Security comparison of the proposed scheme with others.

Schemes/attributes	UIA	PIA	RA	OFGA	SSA	LSA	KSSTIA	LSR	SPC	KKA	PFS	MA	SSKA	UA
Lu et al. (2008)	Yes	No	Yes	No	Yes	NA	No	NA	Yes	Yes	Yes	No	No	No
Xu et al. (2009)	No	No	Yes	No	Yes	No	No	No	Yes	Yes	Yes	No	No	No
Wu et al. (2010)	No	No	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	No	No	No
Debiao et al. (2012)	Yes	No	Yes	No	Yes	No	Yes	No	Yes	Yes	Yes	No	No	No
Wei et al. (2012)	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	Yes	Yes	No	No	No
Wu et al. (2012)	Yes	No	Yes	No	Yes	No	No	No	No	Yes	Yes	Yes	Yes	No
Proposed	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

UIA: Resilience against user impersonation attack; PIA: Resilience against privileged-insider attack; RA: Resilience against replay attack; OFPGA/ONPGA: Resilience against off-line/on-line password guessing attack; SSA: Resilience against server's spoofing attack; LSA: Resilience against lost smartcard attack; KSSTIA: Resilience against known session-specific temporary information attack; LSR: Provides lost smartcard revocation; SPC: Provides secure password change phase; KKA: Resilience against known-key attack; PFS: Provides perfect forward secrecy; MA: Provides mutual authentication; SSKA: Provides secure session key agreement; UA: Provides user's anonymity/secrecy. NA: Not applicable.

Table 4 Computational notations and their descriptions.

Notations	Descriptions
T_{ML}	Time complexity for executing the modular multiplication
T_{EXP}	Time complexity of executing the modular exponentiation operation, $T_{EXP} \approx 240T_{ML}$
T_{INV}	Time complexity for executing the modular inversion operation, $T_{INV} \approx 11.6T_{ML}$
T_H	Time complexity for executing the hash function, which is negligible
T_X	Time complexity for executing the XOR operation, which is negligible

information $ID_a, \sigma_s, e_s, H_a, V_{as}, y, d_a, H(\cdot)$ stored in A's smartcard and derive the password PW_a of A and the secret key x of S, if he/she has the ability to invert the one-way hash function $H(\bullet)$ and solve the DLP. From the Definition 2 and Definition 3, we have $Adv_E^{Hash}(t_1) \leqslant \varepsilon_1$ and $Adv_E^{DLP}(t_2) \leqslant \varepsilon_2$, for any sufficiently small $\varepsilon_1, varepsilon_2 > 0$. Thus it can be concluded that the advantage $Adv2(et_2, q_{R1}, e_{R2})$ is negligible, since it depends on both $Adv_E^{Hash}(t_1)$ and $Adv_E^{DLP}(t_2)$. We can say that the probability of success of E for deriving the password PW_a of A and the secret key x of S is negligible. Therefore, our scheme is provably secure against E for deriving the password PW_a of A and the secret key x of S. □

5.3. Efficiency analysis

In this section, we analyze the functional requirements and computation costs to evaluate the efficiency of our scheme and compared it with others.

5.3.1. Consistency and flexibility

A simple password-based user authentication scheme helps to achieve some basic security requirements and only the server authenticates a remote user. However, this is not the case in many real-life applications (e.g., secret online order placement, online banking tractions) where some sensitive messages are exchanged between user and server, and also authentication of the server is required, otherwise an adversary may impersonate the server to steal user secret information. Our scheme provides mutual authentication, which provides consistency between user and server. Furthermore, mutual authentication is not sufficient to provide the data integrity and confidentiality, a session key negotiation is also important for establishing a secure channel between them. The proposed scheme not only achieves mutual authentication, but also provides a session key agreement, which makes our scheme more flexible for various applications.

Algorithm 2: $Exp2_{DLP,E}^{Hash}$

1: Capture the lost/stolen smartcard and extract the information $ID_a, \sigma_s, e_s, H_a, V_{as}, y, d_a, H(\cdot)$ using the methods proposed in (Kocher et al., 1999; Messerges et al., 2002), where $V_a = H(ID_a||PW_a||d_a)$, $D_s = g^{d_s} \bmod p$, $\sigma_s = d_s - xe_s \bmod p$, $e_s = H(ID_a||D_s||SN)$ and $V_s = H(ID_a||d_s||SN)$
2: Call the *Reveal*1 oracle on input V_a to retrieve ID_a, PW_a and d_a as $(ID_a^*||PW_a^*||d_a^*) \leftarrow Reveal1(V_a)$
3: Call the *Reveal*1 oracle on input e_s to retrieve ID_a, D_s and SN as $(ID_a^{**}||D_s^{**}||SN^{**}) \leftarrow Reveal1(e_s)$
4: Call the *Reveal*2 oracle on input D_s^{**} to retrieve d_s as $(d_s^{**}) \leftarrow Reveal2(D_s^{**})$
5: Compute $x^{**} = e_s^{-1}(d_s^{**} - \sigma_s) \bmod p$
6: If $(ID_a^* = ID_a)$ and $(d_a^* = d_a)$ then
7: Accept PW_a^* as the correct passwordPW_a of A and x^{**} as the secret key x of S
8: Return 1 (Success)
9: Else
10: Return 0 (Failure)
11: End If

5.3.2. Scalability and fairness

In our scheme, a user is free to choose and change his password without remote server's assistance. In addition, our scheme stores user's secret information on the smartcard and the user memorizes his password. These are used to accomplish mutual authentication and session key agreement so that the server does not need to maintain a large password-verification table. Note that each card identifier recorded by the system is

Table 5 Computation cost comparison of the proposed scheme with others.

Schemes/ attributes	Registration phase	Login phase	Mutual authentication phase	Password change phase	Total computation cost	No. of rounds (login & verification phases)
Lu et al. (2008)	$1T_{EXP} + 1T_H$	$1T_{EXP} + 1T_{INV} + 1T_H$	$4T_H$	$2T_{EXP} + 2T_H$	$4T_{EXP} + 1T_{INV} + 8T_H \approx 971.6T_{ML}$	3
Xu et al. (2009)	$1T_{EXP} + 2T_H$	$2T_{EXP} + 3T_H$	$4T_{EXP} + 6T_H$	$2T_{EXP} + 4T_H$	$9T_{EXP} + 15T_H \approx 2160T_{ML}$	2
Wu et al. (2010)	$2T_{EXP} + 1T_{INV} + 1T_H$	$1T_{EXP} + 1T_H$	$3T_{EXP} + 1T_{INV} + 8T_H$	$2T_{EXP} + 2T_{INV}$	$7T_{EXP} + 4T_{INV} + 10T_H \approx 1726.4T_{ML}$	3
Debiao et al. (2012)	$1T_{EXP} + 1T_{INV} + 1T_H$	$1T_{EXP} + 1T_{INV} + 2T_H$	$2T_{EXP} + 1T_{INV} + 7T_H$	$2T_{EXP} + 2T_{INV} + 2T_H$	$6T_{EXP} + 5T_{INV} + 12T_H \approx 1498T_{ML}$	3
Wei et al. (2012)	$1T_{EXP} + 3T_H$	$1T_{EXP} + 2T_H$	$1T_{EXP} + 1T_{INV} + 7T_H$	$2T_H$	$3T_{EXP} + 1T_{INV} + 14T_H \approx 778T_{ML}$	3
Wu et al. (2012)	$1T_X + 2T_H$	$1T_H$	$3T_X + 1T_{INV} + 8T_H$	$1T_H$	$4T_X + 1T_{INV} + 12T_H \approx 11.6T_{ML}$	3
Proposed	$1T_{EXP} + 4T_X + 4T_H$	$2T_{EXP} + 3T_X + 3T_H$	$2T_{EXP} + 1T_X + 5T_H$	$3T_X + 2T_H$	$5T_{EXP} + 9T_X + 14T_H \approx 1200T_{ML}$	2

quite short and the system does not require keeping these card identifiers secret. This approach is cost efficient and secure as compared with maintaining the password table in a traditional remote authentication scheme. Therefore, the server can accommodate a large number of users without compromising user secrecy. Besides, our scheme provides most of the security features and it provides scalability and fairness in secure data transmission over hostile networks.

5.3.3. Comparison of the proposed scheme with others

A security comparison of our scheme with (Lu et al., 2008; Xu et al., 2009; Wu et al., 2010, 2012; Wei et al., 2012; Debiao et al., 2012) is given in Table 3 that shows our scheme protects most of the attacks.

A comparison of our scheme with others is given from the perspective of computational cost efficiency. According to (Islam and Biswas, 2012a,b,c, 2013b,c,d, 2014a,b), the different time complexities and their conversion to the time complexity for executing modular multiplication (T_{ML}) are given in Table 4. The computation cost comparison is given in Table 5 that shows our scheme reduced the computation cost compared to (Xu et al., 2009; Wu et al., 2010; Debiao et al., 2012), but increases the same with respect to (Lu et al., 2008; Wei et al., 2012; Wu et al., 2012). However, our scheme has some limitations such as (1) high computation cost, (2) both the server and the user must be synchronized for timestamp realization; (3) user must have extra ability to store a random number into the smartcard and (4) the memory requirement our scheme is high. To store the information $[\sigma_s, e_s, H_a, V_{as}, y, d_a]$ into the smartcard our scheme needs $3(|p| + |h|)$ bits whereas Wu et al.'s scheme (2012) requires $(|p| + |h|)$ bits for $[N, s]$, where the length of the identity is ignored. Here $|p|$ and $|h|$ represent the bit length of the modulus p and the output length of the hash function $h(\cdot)$. It may be noted that the increased computation cost and limitations of our scheme can be considered quite reasonable with the assurance of better security features.

6. Conclusions

This paper studied Wu et al.'s password-based user authentication scheme for the integrated EPR information system and identified some security weaknesses such as privileged-insider attack, lost smartcard/off-line password guessing attack and known session-specific temporary information attack. Furthermore, it does not support revocation of lost/stolen smartcard and user's anonymity. Also its password change phase is inefficient and inconvenient. Thus, a new two-factor user authentication scheme for the integrated EPR information system is proposed using Chen et al.'s protocol and Schnorr's signature scheme. The security and efficiency analysis of our scheme are made and compared with others, which ensure that our scheme is more secure, consistent, flexible and scalable.

Acknowledgements

The authors are grateful to the Editor-in-Chief, Prof. Mansour M. Alsulaiman and anonymous reviewers for their insightful comments and valuable suggestions which helps us to improve the paper. This research work is supported by the Department

of Science and Technology (DST), Government of India under the **INSPIRE fellowship Ph.D. program** (Grant No. IF10247) and the Department of Information Technology (DIT), Ministry of Communication and Information Technology, Government of India under the **Information Security Education and Awareness (ISEA) program** (Project No. MIT(2)/2006-08/189/CSE). The authors would also like to express their thanks to the Department of Computer Science and Engineering, Indian School of Mines, Dhanbad, India and the Department of Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani, Rajasthan, India for providing their research support, as without their help this work would not have been possible.

References

Blake-Wilson, S., Johnson, D., Menezes, A., 1997. Key agreement protocols and their security analysis. In: Proceedings of the 6th IMA International Conference on Cryptography and Coding, vol. 1355. Springer-Verlag, pp. 30–45.

Canetti, R., Krawczyk, H., 2001. Analysis of key exchange protocols and their use for building secure channels. In: Proceedings of Advances in Cryptology (Eurocrypt'01). Springer-Verlag, pp. 453–474.

Chatterjee, S., Das, A.K., Sing, J.K., 2014. A novel and efficient user access control scheme for wireless body area sensor networks. J. King Saud Univ. Comput. Inf. Sci. 26 (2), 181–201.

Chen, T.-H., Lee, W.-B., Chen, H.-B., 2008. A round-and computation-efficient three-party authenticated key exchange protocol. J. Syst. Software 81, 1581–1590.

Chen, C.-L., Chen, Y.-Y., Chen, Y.-H., 2009. Group-based authentication to protect digital content for business applications. Int. J. Innovative Comput. Inf. Control 5 (5), 1243–1251.

Cheng, Z., Nistazakis, M., Comley, R., Vasiu, L., 2005. On the indistinguishability-based security model of key agreement protocols-simple cases. Cryptology ePrint Archieve, Report 2005/129, 2005.

Das, A.K., Bruhadeshwar, B., 2013. An improved and effective secure password-based authentication and key agreement scheme using smart cards for the telecare medicine information system. J. Med. Syst. 37, 9969–9989.

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

Elberg, P.B., 2001. Electronic patient records and innovation in health care services. Int. J. Med. Informatics 64 (2–3), 201–205.

Fan, C.-I., Chan, Y.-C., Zhang, Z.-K., 2005. Robust remote authentication scheme with smart cards. Comput. Secur. 24, 619–628.

Gritzalis, S., Lambrinoudakis, C., Lekkas, D., Deftereos, S., 2005. Technical guidelines for enhancing privacy and data protection in modern electronic medical environments. IEEE Trans. Inf. Technol. Biomed. 9 (3), 413–423.

Hou, M., Xu, Q., Shanqing, G., Jiang, H., 2010. Cryptanalysis of identity-based authenticated key agreement protocols from parings. J. Networks 5 (7), 826–855.

Huang, C., Lee, H., Lee, D.H., 2011. A privacy-strengthened scheme for E-healthcare monitoring system. J. Med. Syst. 36 (5), 2959–2971.

Islam, S.H., Biswas, G.P., 2011. A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. J. Syst. Software 84 (11), 1892–1898.

Islam, S.H., Biswas, G.P., 2012a. A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile network. Ann. Telecommun. 67 (11–12), 547–558.

Islam, S.H., Biswas, G.P., 2012b. An efficient and provably-secure digital signature scheme based on elliptic curve bilinear pairings. Theor. Appl. Informatics 24 (2), 109–118.

Islam, S.H., Biswas, G.P., 2012c. An improved ID-based client authentication with key agreement scheme on ECC for mobile client-server environments. Theor. Appl. Informatics 24 (4), 293–312.

Islam, S.H., Biswas, G.P., 2013a. Design of improved password authentication and update scheme based on elliptic curve cryptography. Math. Comput. Model. 57 (11–12), 2703–2717.

Islam, S.H., Biswas, G.P., 2013b. Provably secure certificateless strong designated verifier signature scheme based on elliptic curve bilinear pairings. J. King Saud Univ. Comput. Inf. Sci. 25, 51–61.

Islam, S.H., Biswas, G.P., 2013c. Provably secure and pairing-free certificateless digital signature scheme using ECC. Int. J. Comput. Math. 90 (11), 2244–2258.

Islam, S.H., Biswas, G.P., 2013d. An efficient and secure strong designated verifier signature scheme without bilinear pairings. J. Appl. Math. Informatics 31 (3–4), 425–441.

Islam, S.H., Biswas, G.P., 2014a. Provably secure identity-based strong designated verifier proxy signature scheme from bilinear pairings. J. King Saud Univ. Comput. Inf. Sci. 26 (1), 55–67.

Islam, S.H., Biswas, G.P., 2014b. Certificateless short sequential and broadcast multisignature schemes using elliptic curve bilinear pairings. J. King Saud Univ. Comput. Inf. Sci. 26 (1), 89–97.

Khan, M.K., Alghathbar, K., 2010. Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks'. Sensors 10 (3), 2450–2459.

Khan, M.K., Kim, S.-K., Alghathbar, K., 2011. Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme. Comput. Commun. 34 (3), 305–309.

Kocher, P., Jaffe, J., Jun, B., 1999. Differential power analysis. In: Proceedings of the Advances in Cryptology (Crypto'99). Springer-Verlag, pp. 388–397.

Leiner, F., Gaus, W., Haux, R., Knaup-Gregori, P., 2003. Medical Data Management-A Practical Guide. Springer, New York.

Liao, Y.P., Wang, S.S., 2009. A secure dynamic ID based remote user authentication scheme for multi-server environment. Comput. Stand. Interfaces 31, 24–29.

Lu, R., Cao, Z., Chai, Z., Liang, X., 2008. A simple user authentication scheme for grid computing. Int. J. Network Secur. 7 (2), 202–206.

Mandt, T., Tan, C., 2008. Certificateless authenticated two-party key agreement protocols. In: Proceedings of the ASIAN, vol. 4435. Springer-Verlag, pp. 37–44.

Messerges, T.S., Dabbish, E.A., Sloan, R.H., 2002. Examining smart-card security under the threat of power analysis attacks. IEEE Trans. Comput. 51 (5), 541–552.

Schnorr, C.P., 1990. Efficient identification and signatures for smart cards. In: Proceedings of the Advances in Cryptology (Eurocrypt'89), vol. 434. Springer-Verlag, pp. 239–252.

Swanson, C.M., 2008. Security in Key Agreement: Two-Party Certificateless Schemes (Master's thesis). University of Waterloo, Canada.

Vaidya, B., Makrakis, D., Mouftah, H.T., 2010. Improved two-factor user authentication in wireless sensor networks. In: Proceedings of the IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications, pp. 600–606.

Wang, Y.-Y., Liu, J.-Y., Xiao, F.-X., Dan, J., 2009. A more efficient and secure dynamic ID-based remote user authentication scheme. Comput. Commun. 32, 583–585.

Wang, R.C., Juang, W.S., Lei, C.L., 2011. Provably secure and efficient identification and key agreement protocol with user anonymity. J. Comput. Syst. Sci. 77 (4), 790–798.

Wei, J., Hu, X., Liu, W., 2012. An improved authentication scheme for telecare medicine information systems. J. Med. Syst. http://dx.doi.org/10.1007/s10916-012-9835-1.

Wong, K.H.M., Zheng, Y., Cao, J., Wang, S., 2006. A dynamic user authentication scheme for wireless sensor networks. In: Proceedings of the IEEE International Conference on Sensor Network Ubiquitous and Trustworthy Computing, pp. 318–327.

Wu, Z.-Y., Lee, Y.-C., Lai, F., Lee, H.-C., Chung, Y., 2010. A secure authentication scheme for telecare medicine information systems. J. Med. Syst. 36 (3), 1529–1535.

Wu, Z.-Y., Tseng, Y.-J., Chung, Y., Chen, Y.-C., Lai, F., 2011a. A reliable user authentication and key agreement scheme for web-based hospital-acquired infection surveillance information system. J. Med. Syst. 36 (4), 2547–2555.

Wu, S., Zhu, Y., Pu, Q., 2011b. A novel lightweight authentication scheme with anonymity for roaming service in global mobility networks. Int. J. Network Manage 21 (5), 384–401.

Wu, Z.-Y., Chung, Y., Lai, F., Chen, T.-S., 2012. A password-based user authentication scheme for the integrated EPR information system. J. Med. Syst. 36 (2), 631–638.

Xu, J., Zhu, W.-T., Feng, D.-G., 2009. An improved smart card based password authentication scheme with provable security. Comput. Stand. Interfaces 31, 723–728.