J Med Syst (2015) 39: 144
DOI 10.1007/s10916-015-0322-3

SYSTEMS-LEVEL QUALITY IMPROVEMENT

A Hash Based Remote User Authentication and Authenticated Key Agreement Scheme for the Integrated EPR Information System

Chun-Ta Li[1] · Chi-Yao Weng[2] · Cheng-Chi Lee[3,4] · Chun-Cheng Wang[1]

Received: 11 April 2015 / Accepted: 12 August 2015 / Published online: 9 September 2015

Abstract To protect patient privacy and ensure authorized access to remote medical services, many remote user authentication schemes for the integrated electronic patient record (EPR) information system have been proposed in the literature. In a recent paper, Das proposed a hash based remote user authentication scheme using passwords and smart cards for the integrated EPR information system, and claimed that the proposed scheme could resist various passive and active attacks. However, in this paper, we found that Das's authentication scheme is still vulnerable to modification and user duplication attacks. Thereafter we propose a secure and efficient authentication scheme for the integrated EPR information system based on lightweight hash function and bitwise exclusive-or (XOR) operations. The security proof and performance analysis show our new scheme is well-suited to adoption in remote medical healthcare services.

Keywords Integrated EPR information system · User authentication · Key agreement · Hash function · Network security

This article is part of the Topical Collection on *Systems-Level Quality Improvement*

✉ Cheng-Chi Lee
cclee@mail.fju.edu.tw

Chun-Ta Li
th0040@mail.tut.edu.tw

Chi-Yao Weng
cyweng@mail.nptu.edu.tw

[1] Department of Information Management, Tainan University of Technology, No. 529, Zhongzheng Road, Tainan City, 71002, Taiwan

[2] Department of Computer Science, National Pingtung University, No. 4-18, Min-Sheng Road, Pingtung City, 90003, Taiwan

[3] Department of Library and Information Science, Fu Jen Catholic University, No. 510, Jhongjheng Road, New Taipei City, 24205, Taiwan

[4] Department of Photonics and Communication Engineering, Asia University, No. 500, Lioufeng Road, Taichung City, 41354, Taiwan

Introduction

With the rapid development of network and communication technologies, in order to monitor and analyze patients' health, the integrated EPR information system is widely used to share patients' medical histories and help medical institutions to make correct clinical decisions rapidly. The registered user can on-line access various medical information and healthcare services from remote medical server. The ultimate aim of integrated EPR information system is to allow the sharing of patients' medical information and histories scattered among all medical institutions, doctors, and patients through the Internet. Hence, all the medical participants, who could be from hospitals or from clinics and even an individual patient can be free to access all of services within the integrated EPR information systems. Due to the openness of the Internet, the public network communication between remote user and medical server is always a subject of information security and privacy risk in integrated EPR information system as a malicious attacker is considered to be powerful ability to launch various attacks.

With the increase of security attacks [4, 6, 8, 9, 13, 15, 16, 19–21, 23, 25, 29] such as message replaying, participant masquerading and privacy exposing, many smart card based password authentication and key agreement schemes for the integrated EPR information system have been proposed [3, 7, 12, 17, 18, 26, 27].

In 2012, Wu et al. proposed a password based solution to build an efficient and patient-safety-centric scheme [27] for the integrated EPR information system. Wu et al.'s scheme requires only lightweight hashing functions and multiplication computations to be implemented under the medical application environments. However, in 2013, Lee et al. pointed out that Wu et al.'s solution is still vulnerable to lost smart card and stolen verifier attacks. After getting the secrets stored in the smart card by launching power analysis attacks [11, 22], the attacker can easily derives user's password and masquerade as a legitimate user [14]. Lee et al. further proposed an improved version of authentication scheme [12] for the integrated EPR information system and their scheme can provide medical server and remote users with a secure and efficient practical environment. Unfortunately, in 2014, Wen [26] found that Lee et al.'s solution was insecure against off-line password guessing attack if the secrets stored in the user's smart card are compromised and this problem also renders that their scheme fails to prevent user impersonation attack. In order to remedy this security problem found in Lee et al.'s scheme, Wen further proposed an improvement of Lee et al.'s scheme based on quadratic residues [2, 30]. However, in 2015, Das [3] showed that Lee et al.'s scheme and Wen's scheme are still vulnerable to three disadvantages: 1) two schemes have design flaws in password change phase and this irrecoverable error enforces the user to re-register another new smart card issued by the server, 2) two schemes fail to protect privileged insider attack, 3) two schemes does not provide formal security verification. In order to remedy these design flaws in two schemes, Das propose a secure password-based remote user authentication scheme using smart cards for the integrated EPR information system and Das's scheme is also efficient as compared to Lee et al.'s scheme and Wen's scheme.

Although Das's authentication scheme enhanced the security and efficiency of Lee et al.'s scheme and Wen's scheme. However, we found that Das's scheme has two security flaws: 1) the scheme fails to provide synchronized secret by launching modification attacks, 2) the scheme has user duplication attacks in password change phase. In order to solve these security weaknesses, we further propose a more secure user authentication scheme, while retaining the original merits of Das's scheme. Through the formal security proof using the widely-accepted Burrows-Abadi-Needham (BAN) logic analysis [1] and show that our new scheme is surely more suitable than existing ones for use in assisting remote medical services to safeguard patient privacy.

The remainder of the paper is organized as follows. Section "Review of Das's scheme" provides overview of Das's authentication scheme in brief and shows its security weaknesses in Section "Two weaknesses on Das's scheme". Section "The proposed scheme" presents our improved scheme and proves the security of our scheme by using widely-accepted BAN logic analysis in Section "Security proof of our scheme using BAN logic". In Section "Comparison of our scheme with related schemes", we give a detailed comparison between our scheme and other related schemes. Finally, we draw our conclusions in Section "Conclusions".

Review of Das's scheme

In this section, Das's scheme [3] will be briefly reviewed. There are four phases in Das's scheme and Fig. 1 shows the entire flowchart of Das's scheme. For convenience of description, terminology and notations used in the paper are summarized as follows:

- S_j: The trustworthy integrated EPR information system server.
- U_i: The user.
- ID_i: The identity of user U_i.
- PW_i: The password of user U_i.
- $h(\cdot)$: A secure collision-free one-way hash function, such as HMAC [24].
- K: The secret key of S_j, where K is considered as a 1024-bit number.
- H: The constant secret value of S_j, where H is considered as a 1024-bit number.
- X_u: The secret number of U_i, where X_u is considered as a 1024-bit number.
- $||$: The concatenation operation.
- $\oplus$: The bitwise XOR operation.

Registration phase

In this phase, the user U_i registers with the remote server S_j through a secure channel to be a legal user. The details of registration phase are as follows:

Step R1: U_i chooses his/her identity ID_i and password PW_i.

Step R2: U_i generates a random secret number X_u and it is kept secret to the user U_i only.

Step R3: U_i computes $RPW_i = h(X_u||PW_i)$ and sends the registration request $\{ID_i, RPW_i\}$ to S_j via a secure channel.

Step R4: S_j validates the identity ID_i of U_i and computes $v = h(K \oplus ID_i)$ if ID_i is valid.

Step R5: S_j computes $s_1 = h(RPW_i||K)$, $s_2 = h(RPW_i||s_1)$ and $N = v \oplus s_2 \oplus H$.

Step R6: S_j issues a medical smart card containing the information $\{ID_i, h(\cdot), N, s_1\}$ to the user U_i via a secure channel.

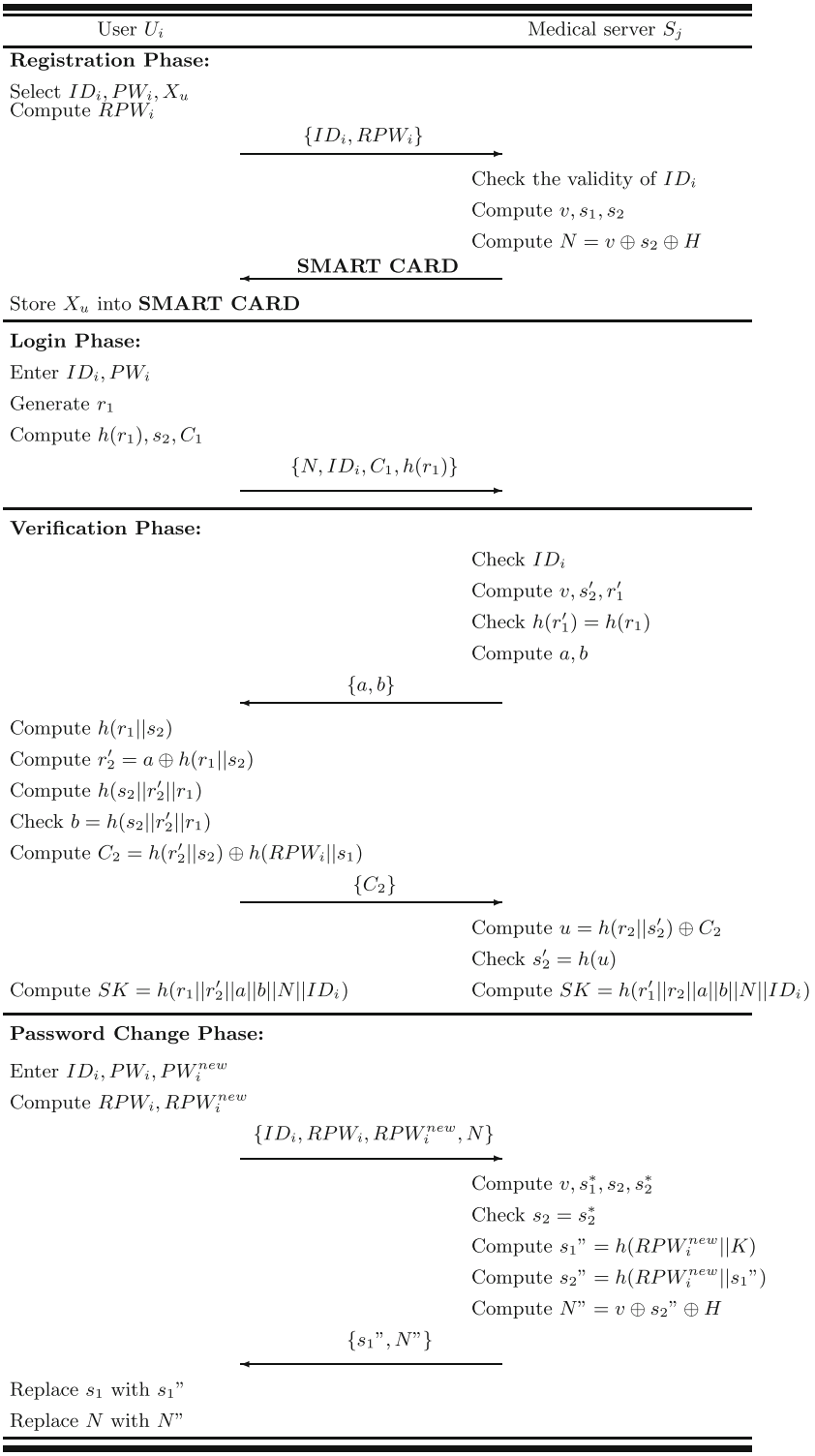

Fig. 1 The flowchart of Das's scheme

After receiving the smart card from S_j, U_i stores X_u in its memory.

Login phase

If U_i wants to access the integrated EPR information system server S_j, the following steps need to be executed:

Step L1: U_i inserts his/her smart card into card reader and inputs identity ID_i and password PW_i. Then smart card computes $RPW_i = h(X_u||PW_i)$.
Step L2: The smart card generates a random number r_1 and computes $h(r_1)$, $s_2 = h(RPW_i||s_1)$ and $C_1 = r_1 \oplus s_2$.
Step L3: Finally, U_i sends the login request message $\{N, ID_i, C_1, h(r_1)\}$ to S_j via a public channel.

Verification phase

When the server S_j receives U_i's login request message, S_j and U_i perform the following steps:

Step V1: S_j verifies the validity of U_i's identity ID_i. If it is valid, S_j goes to Step V2. Otherwise, S_j rejects U_i's login request.
Step V2: S_j computes $v = h(K \oplus ID_i)$, $s_2' = H \oplus N \oplus v$ and $r_1' = s_2' \oplus C_1$ and checks whether $h(r_1') = h(r_1)$. If it holds, S_j stores the pair (ID_i, r_1') in its database and executes Step V3. Otherwise, S_j rejects this login request.
Step V3: S_j computes $a = r_2 \oplus h(r_1'||s_2')$ and $b = h(s_2'||r_2||r_1')$ and sends the authentication request message $\{a, b\}$ to U_i via a public channel, where r_2 is a random number generated by S_j
Step V4: After receiving the message from S_j, U_i computes $h(r_1||s_2)$, $r_2' = a \oplus h(r_1||s_2)$ and $h(s_2||r_2'||r_1)$ and checks whether $b = h(s_2||r_2'||r_1)$. If it holds, U_i successfully authenticates S_j and execute Step V5.
Step V5: U_i computes $C_2 = h(r_{2N||s_2}) \oplus h(RPW_i||s_1)$ and sends the acknowledgement message $\{C_2\}$ to S_j via a public channel.
Step V6: After receiving the message from U_i, S_j computes $u = h(r_2||s_{2N}) \oplus C_2$ and checks whether $s_2' = h(u)$. If it holds, S_j successfully authenticates U_i.
Step V7: Finally, S_j and U_i can compute a secret session key $SK = h(r_1'||r_2||a\ ||b||N||ID_i) = h(r_1||r_2'||a||b||N||ID_i)$ shared between them.

Password change phase

When the user U_i wants to change his/her old password PW_i to a new password PW_i^{new}, U_i must notify the remote server S_j to update the old masked password $RPW_i = h(X_u||PW_i)$ to a new masked password $RPW_i^{new} = h(X_u||PW_i^{new})$.

Step P1: U_i inserts his/her smart card into card reader and inputs identity ID_i, old password PW_i and new password PW_i^{new}. Then smart card computes old masked password $RPW_i = h(X_u||PW_i)$ and new masked password $RPW_i^{new} = h(X_u||PW_i^{new})$ and sends the password change request message $\{ID_i, RPW_i, RPW_i^{new}, N\}$ to S_j via a secure channel.
Step P2: After receiving the request from U_i, S_j computes $v = h(K \oplus ID_i)$, $s_1^* = h(RPW_i||K)$, $s_2 = N \oplus v \oplus H$ and $s_2^* = h(RPW_i||s_1^*)$ and checks whether $s_2 = s_2^*$. If it holds, S_j goes to Step P3. Otherwise, S_j terminates this phase.
Step P3: S_j computes $s_1" = h(RPW_i^{new}||K)$, $s_2" = h(RPW_i^{new}||s_1")$ and $N" = v \oplus s_2" \oplus H$ and sends $\{s_1", N"\}$ to U_i via a secure channel.
Step P4: Finally, U_i replaces s_1 with $s_1"$ and N with $N"$ on his/her medical smart card.

Two weaknesses on Das's scheme

In this section, we show that Das's scheme has two weaknesses, which are discussed in the following subsections.

Modification attacks

In Step V2 of verification phase of Das's scheme, in order to prevent replay attacks and man-in-the-middle attacks, the server stores latest login pair (ID_i, r_1') in its database, where $r_1' = r_1$. Whenever the server S_j receives the next login request message $\{N', ID_i', C_1', h(r_1'')\}$ with new random number r_1'' from the user U_i, S_j further computes $v' = h(K \oplus ID_i')$, $s_2''' = H \oplus N' \oplus v'$ and $r_1''' = s_2''' \oplus C_1'$ and checks whether the stored r_1' matches with the computed r_1'''. If there is a match, S_j discovers that the login request message is a replay message and S_j will reject this request. Otherwise, S_j convinces that the login request is not a replay message and it will replace r_1' with the computed r_1''' in its maintained database.

However, if an attacker U_a intentionally collects previous login request messages over the public channel and replays the previous login request message to S_j, U_a is able to fool server S_j to store wrong pair in its database. To launch modification attack, U_a first collects latest login message $\{N', ID_i', C_1', h(r_1'')\}$ and previous login message $\{N, ID_i, C_1, h(r_1)\}$ from the public channel between U_i and S_j. Note that in previous login session, S_j stores (ID_i, r_i) in its maintained database and S_j will replace previous random number r_i with latest random number r_1'' in latest login session.

Afterwards, U_a can make a fool of medical remote server by replaying the previous login request message $\{N, ID_i, C_1, h(r_1)\}$ to S_j. Since previous login request message $\{N, ID_i, C_1, h(r_1)\}$ is a legal message and $r_1 \neq r_1''$, S_j will remissly replace r_1'' with r_1 in Step V2 of verification phase. Moreover, S_j generates a random number r_2''', computes the pair (a, b) and sends the authentication request message {a, b} to the attacker U_a in Step V3 of verification phase. However, without knowing r_2''', s_2 and $h(RPW_i||s_1)$, the attacker U_a cannot reply the correct acknowledgement message $\{C_2\}$ to S_j in Step V5 of verification phase. As a result, U_a cannot pass the verification of S_j in Step V6 of verification phase and S_j will reject U_a's login request. Although U_a's login request was fail, U_a successfully fooled S_j into believing him/her to store wrong pair in its maintained database. Thus, Das's scheme is vulnerable to the modification attacks.

User duplication attacks

In Das's scheme, we observe that a legitimate user may intentionally duplicate his/her account to multiple non-registered users by using the same identity with different masked passwords and the medical server S_j is not aware of having caused problem. The detailed attacks are described as follows.

(1) In password change of Das's scheme, a registered user U_i can freely change his/her old password PW_i to a new password PW_i^{new} by sending the password change request message $\{ID_i, RPW_i, RPW_i^{new}, N\}$ to remote server S_j via a secure channel, where $RPW_i = h(X_u||PW_i)$ and $RPW_i^{new} = h(X_u||PW_i^{new})$.
(2) After verifying this request message, S_j will compute $s_1" = h(RPW_i^{new}||K)$ and $N" = h(K \oplus ID_i) \oplus s_2" \oplus H$ and send $\{s_1", N"\}$ to U_i, where $s_2" = h(RPW_i^{new}||s_1")$.
(3) Finally, a registered user can successfully duplicate his/her medical account with new information $\{ID_i, h(\cdot), N", s_1", X_u\}$.

Afterwards, U_i has two accounts $\{ID_i, h(\cdot), N, s_1, X_u\}$ and $\{ID_i, h(\cdot), N", s_1", X_u\}$ with same identity and any duplicated account can intentionally expose to other non-registered users. Hence, Das's scheme cannot prevent user duplication attacks.

The proposed scheme

In this section, we propose a simple improvement on Das's authentication scheme, which keeps the merits of original scheme. In order to withstand the user duplication attack that is discussed in Section "User duplication attacks", we use a parameter R to record the number of times U_i re-registers to S_j, where $R = 0$ if it is U_i's initial registration. Fig. 2 shows the entire flowchart of our enhanced scheme for the integrated EPR information system.

Registration phase

In this phase, the user U_i registers with the remote server S_j through a secure channel to be a legal user. The details of registration phase are as follows:

Step R1: U_i chooses his/her identity ID_i and password PW_i.
Step R2: U_i generates a random secret number X_u and it is kept secret to the user U_i only.
Step R3: U_i computes $RPW_i = h(X_u||PW_i)$ and sends the registration request $\{ID_i, RPW_i\}$ to S_j via a secure channel.
Step R4: S_j validates the identity ID_i of U_i and computes $v = h(K \oplus ID_i \oplus R)$ if ID_i is valid, where R means the number of times U_i re-registers to S_j.
Step R5: S_j computes $s_1 = h(RPW_i||K)$, $s_2 = h(RPW_i||s_1)$ and $N = v \oplus s_2 \oplus H$.
Step R6: S_j issues a medical smart card containing the information $\{ID_i, h(\cdot), N, s_1\}$ to the user U_i via a secure channel. Moreover, S_j maintains the access control table for a registration service and the format of access control table is shown in Table 1. Note that the first field records U_i's identity, the second field records *null* if it is U_i's initial registration, and the third field records $R = 0$ if it is U_i's initial registration, otherwise, S_j sets $R = R + 1$ in the existing field for U_i.
Step R7: After receiving the smart card from S_j, U_i stores X_u in its memory.

Login phase

In this phase, the executed steps are the same as Das's scheme.

Verification phase

When the server S_j receives U_i's login request message, S_j and U_i perform the following steps:

Step V1: S_j verifies the validity of U_i's identity ID_i. If it is valid, S_j goes to Step V2. Otherwise, S_j rejects U_i's login request.
Step V2: S_j retrieves the stored R in the access control table and computes $v = h(K \oplus ID_i \oplus R)$, $s_2' = H \oplus N \oplus v$ and $r_1' = s_2' \oplus C_1$. Then, S_j checks whether $h(r_1') = h(r_1)$. If it holds, S_j executes Step V3. Otherwise, S_j rejects this login request. Note that S_j does not store r_1' into the access control table in this step.

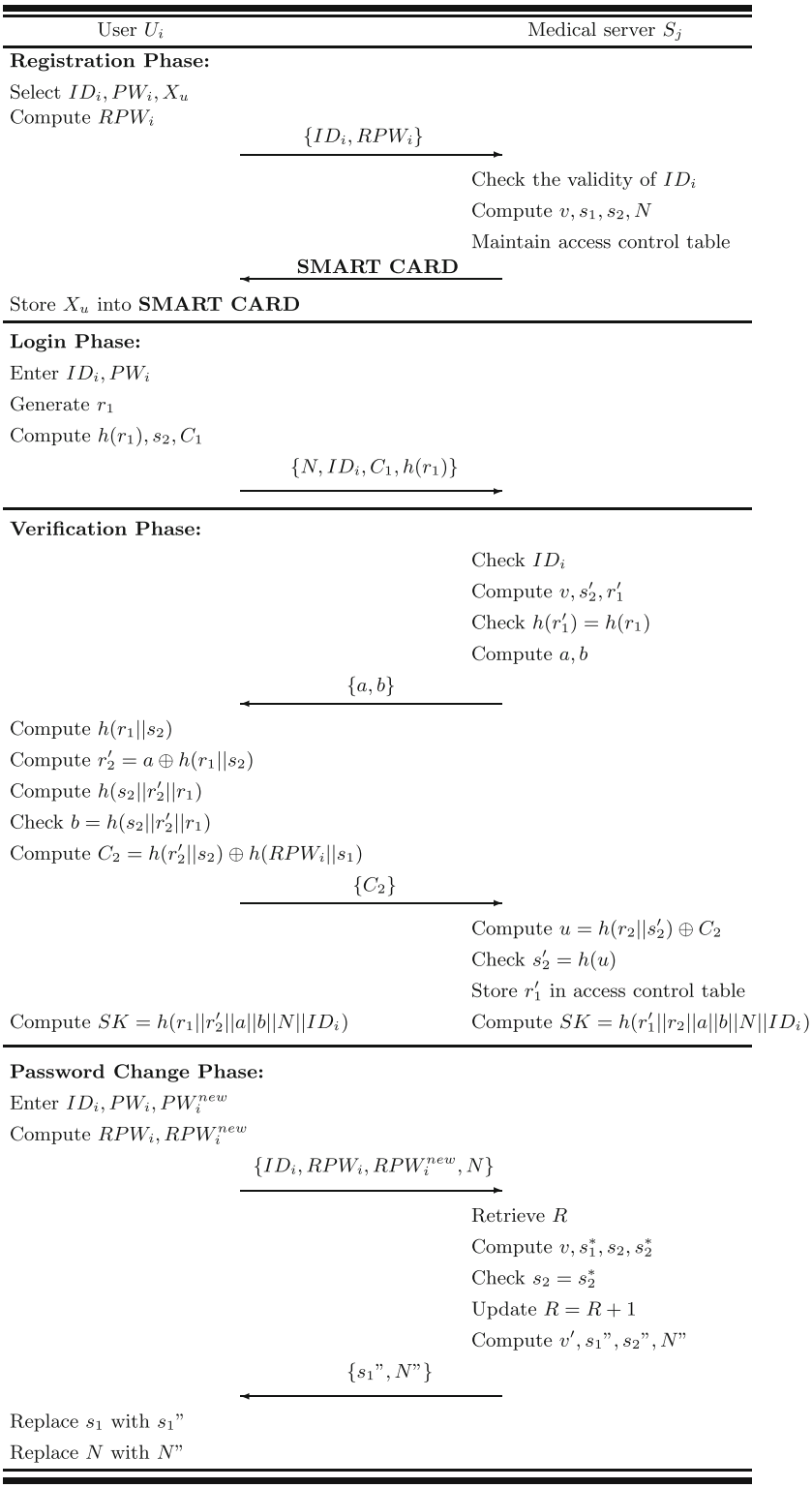

Fig. 2 The flowchart of our proposed scheme

Step V3, Step V4, Step V5: These three steps are the same as Das's scheme.

Step V6: After receiving the message from U_i, S_j computes $u = h(r_2||s_2') \oplus C_2$ and checks whether $s_2' = h(u)$. If it holds, S_j successfully authenticates U_i and stores r_1' in its access control table. After finishing this step, the current format of access control table is shown in Table 2.

Table 1 Access control table of S_j after finishing the registration phase

User identity	Latest login number	Registration times
⋮	⋮	⋮
ID_i	$null$	$R = 0$
⋮	⋮	⋮

Step V7: This step is the same as Das's scheme.

In order to resist modification attacks, in Step V6 of verification phase, the server S_j will store the latest random number r_1' in its access control table after verifying U_i's acknowledgement message C_2. For such design of our scheme, an attacker U_a cannot simply replay the previous login request messages to S_j to launch modification attacks due to U_a cannot compute the correct acknowledgement message C_2 without knowing r_2', s_2, RPW_i and s_1. In this way, the server confirms that the login request message is certainly a replay message and S_j will discard that message. Thus, our proposed scheme has the ability to prevent the modification attacks.

Password change phase

When the user U_i wants to change his/her old password PW_i to a new password PW_i^{new}, U_i must notify the remote server S_j to update the old masked password $RPW_i = h(X_u||PW_i)$ to a new masked password $RPW_i^{new} = h(X_u||PW_i^{new})$.

Step P1: U_i inserts his/her smart card into card reader and inputs identity ID_i, old password PW_i and new password PW_i^{new}. Then smart card computes old masked password $RPW_i = h(X_u||PW_i)$ and new masked password $RPW_i^{new} = h(X_u||PW_i^{new})$ and sends the password change request message $\{ID_i, RPW_i, RPW_i^{new}, N\}$ to S_j via a secure channel.

Step P2: After receiving the request from U_i, S_j retrieves the stored R in the access control table and computes $v = h(K \oplus ID_i \oplus R)$, $s_1^* = h(RPW_i||K)$, $s_2 = N \oplus v \oplus H$ and $s_2^* = h(RPW_i||s_1^*)$. Then, S_j checks whether $s_2 = s_2^*$.

Table 2 Access control table of S_j after finishing the verification phase

User identity	Latest login number	Registration times
⋮	⋮	⋮
ID_i	r_1'	$R = 0$
⋮	⋮	⋮

If it holds, S_j goes to Step P3. Otherwise, S_j terminates this phase.

Step P3: S_j computes $v' = h(K \oplus ID_i \oplus R + 1)$, $s_1" = h(RPW_i^{new}||K)$, $s_2" = h(RPW_i^{new}||s_1")$ and $N" = v' \oplus s_2" \oplus H$ and sends $\{s_1", N"\}$ to U_i via a secure channel. After finishing this step, the current format of access control table is shown in Table 3.

Step P4: Finally, U_i replaces s_1 with $s_1"$ and N with $N"$ on his/her medical smart card.

Table 3 Access control table of S_j after finishing the password change phase

User identity	Latest login number	Registration times
⋮	⋮	⋮
ID_i	r_1'	$R = R + 1$
⋮	⋮	⋮

In order to prevent user duplication attacks, in Step P3 of password change phase, the value of R is incremented by one and it is updated in S_j's access control table. It is noted that the new parameter $v' = h(K \oplus ID_i \oplus R + 1)$ and it is integrated with new login parameter $N" = v' \oplus s_2" \oplus H$. Although U_i has two accounts $\{ID_i, h(\cdot), N, s_1, X_u\}$ and $\{ID_i, h(\cdot), N", s_1", X_u\}$ with same identity, S_j will compute new parameter $v' = h(K \oplus ID_i \oplus R + 1)$ and verify the validity of $N"$. In this way, U_i cannot use this account $\{ID_i, h(\cdot), N, s_1, X_u\}$ to login to S_j due to the previous login parameter $N = h(K \oplus ID_i \oplus R) \oplus s_2 \oplus H$ is illegal. Finally, any legitimate user cannot launch user duplication attacks in our proposed scheme.

Security proof of our scheme using BAN logic

In this section, we use the BAN logic [1] to analyze the security of the session key between user U_i and medical server S_j. Some notations used in BAN logic analysis are described as follows:

- $A| \equiv X$: It means that A believes the formula X is true.
- $A \lhd X$: It means that A sees the formula X.
- $A| \Rightarrow X$: It means that A has complete control over the formula X.
- $A| \sim X$: It means that A has once said the formula X.
- $\sharp(X)$: It means that X is fresh. The formula X has not been used before or X is a nonce.
- $A \overset{K}{\longleftrightarrow} B$: It means that principals A and B may use the shared key K to communicate. Note that K will never be discovered by any principals except A and B.

– $< X >_Y$: It means that formula X is combined with a secret parameter Y.
– $(X)_K$: It means that formula X is hashed with a key K.
– $\frac{Rule1}{Rule2}$: It can infer $Rule2$ from $Rule1$. For example, $\frac{A creats random X}{A|\equiv\sharp(X)}$ means that principal A creates X, so A believes X is fresh.
– SK: A session key established in each session.

In order to describe logical postulates of BAN logic in formal terms, we list four rules as follows:

(Rule 1) Message meaning rule: $\frac{A|\equiv A \overset{K}{\longleftrightarrow} B, A\lhd(X)_K}{A|\equiv B|\sim X}$

If A believes that K is shared with B and sees X hashed with K, then A believes that B once said X.

(Rule 2) Nonce verification rule: $\frac{A|\equiv\sharp(X), A|\equiv B|\sim X}{A|\equiv B|\equiv X}$

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

(Rule 3) The jurisdiction rule: $\frac{A|\equiv B|\equiv X, A|\equiv B|\Rightarrow X}{A|\equiv X}$

If A believes that B has jurisdiction over X, and A believes that B believes a message X, then A believes X.

(Rule 4) The freshness conjuncatenation rule: $\frac{A|\equiv\sharp(X)}{A|\equiv\sharp(X,Y)}$

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

According to the analytic procedures of BAN logic, two participators U_i and S_j cooperatively run the proposed scheme and we list the verification goals of our scheme as follows:

(G.1): $U_i| \equiv U_i \overset{SK}{\longleftrightarrow} S_j$

(G.2): $S_j| \equiv U_i \overset{SK}{\longleftrightarrow} S_j$

Next, we use BAN logic to transform our scheme, illustrated in Fig. 2 into the idealized form. The scheme generic types are shown in the following:

Message 1. $U_i \rightarrow S_j : N, ID_i, C_1, h(r_1)$
Message 2. $S_j \rightarrow U_i : a, b$
Message 3. $U_i \rightarrow S_j : C_2$

Idealize form of the proposed scheme:

Message 1. $U_i \rightarrow S_j : (s_2)_{v,H}, ID_i, < r_1 >_{s_2}, h(r_1)$
Message 2. $S_j \rightarrow U_i :< r_2 >_{(r_1)_{s_2}}, (r_1, r_2)_{s_2}$
Message 3. $U_i \rightarrow S_j :< s_2 >_{(r_2)_{s_2}}$

To analyze the proposed scheme, the following assumptions are also required:

(A.1): $U_i| \equiv \sharp(r_1)$
(A.2): $S_j| \equiv \sharp(r_2)$
(A.3): $U_i| \equiv \left(U_i \overset{v}{\longleftrightarrow} S_j\right)$
(A.4): $S_j| \equiv \left(U_i \overset{v}{\longleftrightarrow} S_j\right)$
(A.5): $U_i| \equiv \left(U_i \overset{H}{\longleftrightarrow} S_j\right)$
(A.6): $S_j| \equiv \left(U_i \overset{H}{\longleftrightarrow} S_j\right)$
(A.7): $U_i| \equiv S_j| \equiv \left(U_i \overset{v}{\longleftrightarrow} S_j\right)$
(A.8): $S_j| \equiv U_i| \equiv \left(U_i \overset{v}{\longleftrightarrow} S_j\right)$
(A.9): $U_i| \equiv S_j| \equiv \left(U_i \overset{H}{\longleftrightarrow} S_j\right)$
(A.10): $S_j| \equiv U_i| \equiv \left(U_i \overset{H}{\longleftrightarrow} S_j\right)$

Based on the above-mentioned assumptions, the preliminary procedures of BAN logic are well prepared and we show the main steps of the verification proof as follows:

According to the Message 1, we could obtain:

(V.1): $S_j \lhd (s_2)_{v,H}, ID_i, < r_1 >_{s_2}, h(r_1)$

According to the assumption (A.4) and (A.6), we apply the message meaning rule to obtain:

(V.2): $S_j| \equiv U_i| \sim v, H$

According to the assumption (V.2), we apply the message meaning rule to obtain:

(V.3): $S_j| \equiv U_i| \sim s_2$

According to the assumption (V.3), we apply the message meaning rule to obtain:

(V.4): $S_j| \equiv U_i| \sim r_1$

According to the assumption (A.1) and (V.4), we apply the freshness conjuncatenation rule to obtain:

(V.5): $S_j\sharp < r_1 >_{s_2}$

According to (V.4) and (V.5), we apply the nonce verification rule to obtain:

(V.6): $S_j| \equiv U_i| \equiv < r_1 >_{s_2}$

According to (V.3) and (V.6), we apply the jurisdiction rule to obtain:

(V.7): $S_j| \equiv r_1$

According to the Message 2, we could obtain:

Table 4 Performance comparisons of our enhanced scheme with some authentication schemes for the integrated EPR information systems

Schemes ⇒	Hao et al.'s [5]	Jiang et al.'s [10]	Das's [3]	Our proposed
	(2013)	(2014)	(2015)	scheme
$F1$	$2T_c$+$2T_s$+$3T_h$	$3T_c$+$1T_s$+$2T_h$	$7T_h$	$7T_h$
$F2$	$2T_c$+$3T_s$+$2T_h$	$3T_c$+$2T_s$+$1T_h$	$7T_h$	$7T_h$
$F3$	65.9 ms	97.45 ms	1.4 ms	1.4 ms
$F4$	66.15 ms	97.7 ms	1.4 ms	1.4 ms
$F5$	132.05 ms	195.15 ms	2.8 ms	2.8 ms
$F6$	Yes	Yes	Yes	Yes
$F7$	No	No	Yes	Yes
$F8$	Yes	Yes	No	Yes
$F9$	No	No	No	Yes
$F10$	No	No	Yes	Yes

(V.8): $U_i \lhd < r_2 >_{(r_1)_{s_2}}, (r_1, r_2)_{s_2}$

According to the assumption (V.3) and (A.2), we apply the message meaning rule to obtain:

(V.9): $U_i| \equiv S_j| \sim r_2$

According to the assumption (A.2), we apply the freshness conjuncatenation rule to obtain:

(V.10): $U_i\sharp < r_2 >_{(r_1)_{s_2}}$

According to (V.9) and (V.10), we apply the nonce verification rule to obtain:

(V.11): $U_i| \equiv S_j| \equiv < r_2 >_{(r_1)_{s_2}}$

According to (V.9) and (V.11), we apply the jurisdiction rule to obtain:

(V.12): $U_i| \equiv r_2$

According to $SK = h(r_1, r_2, < r_2 >_{(r_1)_{s_2}}, (r_1, r_2)_{s_2}, (s_2)_{v,H}, ID_i)$, (V.12), and (A.1), we could obtain:

(V.13): $U_i| \equiv U_i SK \longleftrightarrow S_j$ (G.1)

According to the Message 3, we could obtain:

(V.14): $S_j \lhd < s_2 >_{(r_2)_{s_2}}$

According to $SK = h(r_1, r_2, < r_2 >_{(r_1)_{s_2}}, (r_1, r_2)_{s_2}, (s_2)_{v,H}, ID_i)$, (V.3), (V.7) and (A.2), we could obtain:

(V.15): $S_j| \equiv U_i SK \longleftrightarrow S_j$ (G.2)

Finally, inferring from formulas V.13 and V.15, we have proven the proposed scheme achieves the verification goals as well as establishes a common session key SK between U_i and S_j.

Comparison of our scheme with related schemes

In this section, we compare our proposed scheme with some smart card based authentication schemes [3, 5, 10] in terms of computation overhead and security properties. For example in the experiment environment (CPU: 3.2 GHz, RAM: 3.0 G), we have followed the experimental results perform in [28]. The result reported that the average time of executing one hash function, one symmetric en/decryption operation and one chaotic maps operation are 0.2 ms, 0.45 ms and 32.2 ms, respectively. Comparison is done only for login and verification phases because these phases are used frequently. Note that exclusive-or operation is negligible and we omit the cost of exclusive-or operation. For convenience to evaluate the computational costs and functional features, we define some notations as follows.

- T_h: The time of executing a one-way hash function.
- T_s: The time of executing a symmetric en/decryption operation.
- T_c: The time of executing a Chebyshev chaotic maps operation.
- $F1$: Computation cost of the user U_i.
- $F2$: Computation cost of the server S_j.
- $F3$: Execution time in user side.
- $F4$: Execution time in server side.
- $F5$: Total execution time.
- $F6$: Provision of session key agreement.
- $F7$: Provision of formal security proof.
- $F8$: Prevention of modification attack.
- $F9$: Prevention of user duplication attack.
- $F10$: Without using synchronized timestamp.

Table 4 shows the comparisons of proposed scheme with related schemes in terms of computation overhead and security properties. As can be seen in Table 4, our scheme and Das's scheme have better performance than other schemes. With respect to the security properties, while Das's scheme

is vulnerable to modification attack, Hao et al.'s scheme and Jiang et al.'s scheme are resistant to the attack. However, the security of Hao et al.'s scheme and Jiang et al.'s scheme were not proved in a formal model, while our proposed scheme not only satisfies all the security attributes but also provides the rigorous proof of the security. From an implementation point of view, our scheme requires less computational power and achieves more security criteria compared with related schemes and these features make our solution quite suitable to resource-constrained environments such as telecare medicine information systems and the integrated EPR information systems.

Conclusions

In this paper, we have analyzed that a smart card based authenticated key agreement scheme for the integrated EPR information system proposed by Das in 2015. Although the security of this scheme was proved through AVISPA tool, we have demonstrated that any legitimate but malicious user was able to launched user duplication attack. Moreover, Das's scheme is vulnerable to modification attack and the malicious attacker can replay the previous login messages to fool medical server into maintaining wrong information in its database. To address these problems, an improved smart card based user authentication and key agreement scheme was presented in this paper. According to the formal verification, the proposed scheme has protected system security during the healthcare delivery session, and is more efficient and practical for the real life healthcare applications.

Acknowledgments The authors would like to thank the anonymous referees for their valuable suggestions and comments. In addition, this paper was supported by the Ministry of Science and Technology, Taiwan, R.O.C., under contract no.: MOST 104-2221-E-165-004 and MOST 104-2221-E-030-002.

References

1. Burrows, M., Abadi, M., Needham, R., A logic of authentication. *ACM Trans. Comput. Syst.* 8(1):18–36, 1990.
2. Chen, Y., Chou, J.S., Sun, H.M., A novel mutual authentication scheme based on quadratic residues for RFID systems. *Computer Networks* 52(12):2373–2380, 2008.
3. Das, A.K., A secure and robust password-based remote user authentication scheme using smart cards for the integrated EPR information system. *Journal of Medical Systems* 39(3):25, 2015.
4. Guo, P., Wang, J., Li, B., Lee, S., A variable threshold-value authentication architecture for wireless mesh networks. *Journal of Internet Technology* 15(6):929–936, 2014.
5. Hao, X., Wang, J., Yang, Q., Yan, X., Li, P., A chaotic map-based authentication scheme for telecare medicine information systems. *Journal of Medical Systems* 37(2):9919, 2013.
6. He, D., Zhang, Y., Chen, J., Cryptanalysis and improvement of an anonymous authentication protocol for wireless access networks. *Wirel. Pers. Commun.* 74(2):229–243, 2014.
7. He, D., Kumar, N., Chilamkurti, N., Lee, J.H., Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol. *Journal of Medical Systems* 38(10):116, 2014.
8. He, D., Kumar, N., Chilamkurti, N., A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks. *Inf. Sci.*, 2015. doi:10.1016/j.ins.2015.02.010.
9. He, D., and Zeadally, S., Authentication protocol for ambient assisted living system. *IEEE Commun. Mag.* 35(1):71–77, 2015.
10. Jiang, Q., Ma, J., Lu, X., Tian, Y., Robust chaotic map-based authentication and key agreement scheme with strong anonymity for telecare medicine information systems. *Journal of Medical Systems* 38(2):12, 2014.
11. Kocher, P., Jaffe, J., Jun, B.: Differential power analysis, in Proceedings of Advances in Cryptology, 1999.
12. Lee, T.F., Chang, I.P., Lin, T.H., Wang, C.C., A secure and efficient password-based user authentication scheme using smart cards for the integrated EPR information system. *J. Med. Syst.* 37(3):9941, 2013.
13. Li, C.T., and Hwang, M.S., An efficient biometrics-based remote user authentication scheme using smart cards. *J. Netw. Comput. Appl.* 33(1):1–5, 2010.
14. Li, C.T., and Lee, C.C., A robust remote user authentication scheme using smart card. *Information Technology and Control* 40(3):236–245, 2011.
15. Li, C.T., and Lee, C.C., A novel user authentication and privacy preserving scheme with smart cards for wireless communications. *Math. Comput. Model.* 55(1-2):35–44, 2012.
16. Li, C.T., Lee, C.C., Weng, C.Y., An extended chaotic maps based user authentication and privacy preserving scheme against DoS attacks in pervasive and ubiquitous computing environments. *Nonlinear Dynamics* 74(4):1133–1143, 2013.
17. Li, C.T., Lee, C.C., Weng, C.Y., A secure chaotic maps and smart cards based password authentication and key agreement scheme with user anonymity for telecare medicine information systems. *Journal of Medical Systems* 38(9):77, 2014.
18. Li, C.T., Weng, C.Y., Lee, C.C., A secure RFID tag authentication protocol with privacy preserving in telecare medicine information systems. *J. Med. Syst.* 39(8):77, 2015.
19. Li, C.T., Lee, C.W., Shen, J.J., An extended chaotic maps based keyword search scheme over encrypted data resist outside and inside keyword guessing attacks in cloud storage services. *Nonlinear Dynamics* 80(3):1601–1611, 2015.
20. Li, W.T., Ling, C.H., Hwang, M.S., Group rekeying in wireless sensor networks: a survey. *International Journal of Network Security* 16(6):401–410, 2014.
21. Liao, I.E., Lee, C.C., Hwang, M.S., A password authentication scheme over insecure networks. *J. Comput. Syst. Sci.* 72(4):727–740, 2006.
22. Messerges, T.S., Dabbish, E.A., Sloan, R.H., Examining smart-card security under the threat of power analysis attacks. *IEEE Trans. Commun.* 51(5):541–552, 2002.
23. Ramasamy, R., and Muniyandi, A.P., An efficient password authentication scheme for smart card. *International Journal of Network Security* 14(3):180–186, 2012.
24. RFC 2104 − HMAC. Keyed-hashing for message authentication. ⟨http://www.ietf.org/rfc/rfc2104.txt⟩.

25. Shen, J., Tan, H., Wang, J., Wang, J., Lee, S., A novel routing protocol providing good transmission reliability in underwater sensor networks. *Journal of Internet Technology* 16 (1):171–178, 2015.
26. Wen, F., A more secure anonymous user authentication scheme for the integrated EPR information system. *J. Med. Syst.* 38:42, 2014.
27. Wu, Z.Y., Chung, Y.F., Lai, F., Chen, T.S., A password-based user authentication scheme for the integrated EPR information system. *J. Med. Syst.* 36(2):631–638, 2012.
28. Xue, K., and Hong, P., Security improvement on an anonymous key agreement protocol based on chaotic maps. *Commun. Nonlinear Sci. Numer. Simul.* 17(7):29691V2977, 2012.
29. Yang, L., Ma, J.F., Jiang, Q., Mutual authentication scheme with smart cards and password under trusted computing. *International Journal of Network Security* 14(3):156–163, 2012.
30. Yeh, T.C., Wu, C.H., Tseng, Y.M., Improvement of the RFID authentication scheme based on quadratic residues. *Comput. Commun.* 34(3):337–341, 2011.