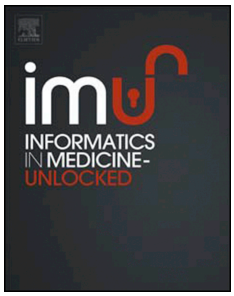
Accepted Manuscript



An efficient and secure remote user mutual authentication scheme using smart cards for Telecare medical information systems

Niranchana Radhakrishnan, Marimuthu Karuppiah

PII: S2352-9148(17)30169-7

DOI: 10.1016/j.imu.2018.02.003

Reference: IMU 92

To appear in: *Informatics in Medicine Unlocked*

Received Date: 22 September 2017

Revised Date: 31 January 2018

Accepted Date: 7 February 2018

Please cite this article as: Radhakrishnan N, Karuppiah M, An efficient and secure remote user mutual authentication scheme using smart cards for Telecare medical information systems, *Informatics in Medicine Unlocked* (2018), doi: 10.1016/j.imu.2018.02.003.

Revisions for the Reviewers' Comments

Manuscript Number: IMU-2017-157
Title: An Efficient and Secure Remote User Mutual Authentication Scheme using Smart Cards for Telecare Medical Information Systems

Informatics in Medicine Unlocked

The authors would like to thank the reviewers and the Editor for their valuable suggestions that resulted in the improvement of the quality, correctness, presentation and readability of the revised paper (IMU-2017-157). We have taken all the comments into consideration in the revised manuscript as follows. We hope these revisions will meet the reviewers' requirements.

Reviewer #1:

- Abstract is general. So authors clearly mention about Lee et al. scheme.
  ✓Thank you for your valuable suggestion. We have clearly mentioned about Lee et al. scheme in abstract itself.

- Provide the formal analysis either by Proverif or BAN logic.
  ✓Thank you for your valuable suggestion. As per reviewer direction, we have provided the formal proof using Random Oracle model. Please refer the page No.18(section 6.1)

- Proposed scheme compared with recent schemes (2016 and 2017).
  ✓Thank you for your valuable suggestion. As per reviewer direction, we have added few recent related works. Please find the referec [64], [65] and [68].

Reviewer #2

- First of all, the authors fail to conduct a good survey of recent related works. Only few works published in the recent two years have been considered, and many important recently published works are overlooked. Need to cite recent works.
  ✓Thank you for your valuable suggestion. We have added few recent related works. Please find the referec [64], [65] and [68].

- No need to strike out the equation since researchers can confuse.
  ✓Thank you for your valuable suggestion. We have removed the strike out mark.

- Authors must provide diagrammatic flow diagram for Lee et al. scheme.
  ✓Thank you for your valuable suggestion. Please refer the figure 2(PP. 9).

- Need to check the grammatical errors.
  ✓Thank you for your valuable suggestion. We have checked the typo erors carefully throughout the paper.

Reviewer #3

- The information of some of the used notations is missing it should be added in Table 2.
  ✓Thank you for your valuable suggestion. We have added symbols in Table 2(pp. 6).
- Provide a flow chart in order to explain the working of the proposed scheme.
  ✓Thank you for your valuable suggestion. Please refer the figure 3 and 4(PP. 15 and 17).
- My biggest concern is with the security analysis of the proposed scheme. Provide the formal security analysis of the proposed scheme using some of the standard model such as ROR (real-or-random). Also provide the formal security verification of the proposed scheme using AVISPA tool.
  ✓Thank you for your valuable suggestion. As per reviewer direction, we have provided the formal proof using Random Oracle model. Please refer the page No.18(section 6.1).
- The proposed scheme is compared only with two schemes. I think it should be compared with more recent related existing schemes.
  ✓Thank you for your valuable suggestion. The proposed scheme is compared with the recent schemes. Please refer the Table 3, 4 and 5.
- Remove the typos and grammar mistakes from the paper.
  ✓Thank you for your valuable suggestion. We have checked the typo erors carefully throughout the paper.
- Location information is missing in some of the references i.e., [55] D. V. Klein, Foiling the cracker: A survey of, and improvements to, password security, in: Proceedings of the 2nd USENIX Security Workshop, 1990, pp. 514.
  ✓Thank you for your valuable suggestion. We have mentioned the location of the conference. Please refer the reference [52].

Reviewer #4

- However, the authors should have made comparison analysis against some more schemes including the one [31] contributed by the authors.
  ✓Thank you for your appreciations and suggestions. The proposed scheme is compared with the recent schemes. Please refer the Table 3, 4 and 5.
- Number of self citations is to limited
  ✓Thank you for your valuable suggestion. As per the direction, the self citations is removed.

Finally, we hope the above revisions will meet the reviewers' requirements.

An Efficient and Secure Remote User Mutual Authentication Scheme using Smart Cards for Telecare Medical Information Systems

Niranchana Radhakrishnan, Marimuthu Karuppiah*

School of Computer Science and Engineering, Vellore Institute of Technology(VIT), Vellore-632014, Tamilnadu, India.

Abstract

Authentication schemes are widely used mechanisms to thwart unauthorized access of resources over insecure networks. Several smart card based password authentication schemes for Telecare Medical Information Systems (TMIS) have been proposed in the literature. Recently, Lee et al. proposed an authentication scheme for TMIS and then they claimed that their scheme is able to resist various attacks. However, in this paper we demonstrate that Lee et al. scheme is still vulnerable to forgery and offline password guessing attacks and it is also unable to provide user anonymity, forward secrecy and mutual authentication. With the intention of fixing the weaknesses of Lee et al. scheme, we present a secure authentication scheme for TMIS. Moreover, the proposed scheme can also resist all known attacks. We prove the security of the proposed scheme with the help of widely-accepted random Oracle model. Finally, we carry out the performance evaluation of the proposed scheme and other related schemes, and the result favors that the proposed scheme provides better trade-off among security and performance as compared to other existing related schemes.

Keywords: User impersonation attack, Password authentication, Off-line password guessing attack, User anonymity, TMIS

*Corresponding author

Email address: mailtoniranch@gmail.com, marimuthume@gmail.com (Niranchana Radhakrishnan, Marimuthu Karuppiah)

1. Introduction

Healthcare systems are among the latest to join the trend of shifting to a digital environment due to the ease of management, increased efficiency etc. This has been made feasible due to the recent breakthroughs in the domains of communication and technology. Thus, the process of setting up a health appointment has been made obsolete. Digitizing the entire process has ushered in efficient, prompt and high quality medical services.

The new systems provide many advantages i) like the ease of access to medical records, less maintenance[1, 2]; ii) integration of patient's medical records from diverse medical service providers[3, 4]; iii) providing remote care[5, 6] etc. The cardinal aim of this system is to provide reliable and convenient medical services to the patient. The telecare medical information system (TMIS) enables the deliverance of such services. The architecture of user authentication for TMIS is shown in Figure 1.

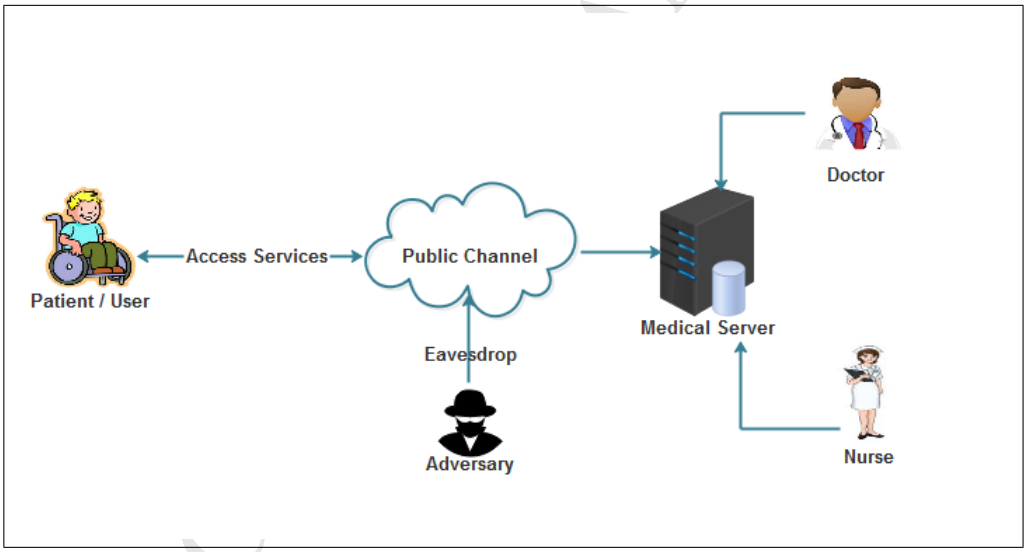


Figure 1: The architecture of user authentication for TMIS

In TMIS, the medical server maintains a database which keeps the electronic medical records(EMR) of its registered patients (users) and makes certain healthcare services available to them whenever requested. Thus, an issue pertaining to data protection of sensitive medical records is of utmost importance. It is the server's responsibility to ensure the integrity of health data that is transferred to the user's computing device[7]. Therefore, there

is a need for remote authentication so that the server authenticates the validity of users (patients), before granting them access to sensitive data and resources.

Several user authentication schemes[8, 9, 10, 11, 12, 13, 14, 15, 16, 17] have been presented for TMIS in the past few years. Wu et al.[10] proposed an authentication scheme and claimed that their scheme was apt for TMIS in 2010. However, He et al.[11] proved that Wu et al.'s scheme not resist insider and impersonation attacks. He et al. then proposed their improved scheme. Nevertheless, Wei et al.[12] proved that schemes in [10, 11] were susceptible to off-line password guessing attack. In order to fix these flaws, Wei et al. proposed a scheme and claimed that their scheme is secure. Though, Zhu et al.[13] demonstrated the scheme of Wei et al. is vulnerable to off-line password guessing attack. They then presented an enhanced authentication scheme. Later, Lee et al.[14] examined the flaws of the authentication schemes in [10, 12] and [13], and proposed an enhanced scheme to resist some well-known attacks. Besides, Chen et al.[8] proved that the scheme of Khan et al.[18] is vulnerable to insider attack and proposed an enhanced scheme to fix the security weaknesses in [18].

Recently, Jiang et al. [15] showed that the scheme in [8] is vulnerable to identity guessing attack and consequently presented their enhanced scheme. Furthermore, Xie et al.[17] and Lin [16] showed that the scheme in [8] is susceptible to dictionary attacks, impersonation attacks and off-line password guessing attacks. They then presented their improved authentication schemes for TMIS. Later, Cao et al. [9] also showed that the scheme[8] permitted the attacker to differentiate patients in dissimilar login sessions and that the server required to perform an exhaustive search of the account database. To fix the drawbacks of [8], they then proposed an enhanced scheme for TMIS. Besides, Lee et al.[19] proved that the scheme of Wu et al.[20] is still vulnerable to stolen verifier and smart card lost attacks and proposed an enhanced scheme to fix the security weaknesses in [20].

1.1. Our contribution

In this paper, first, we have shown that Lee et al.[19] does not meet the user anonymity, and mutual authentication property. Additionally, it is open to insider, offline password guessing, user impersonation and Denial of service(DoS) attacks. Next, with the purpose of fixing the weaknesses of Lee et al.s scheme, we have presented an enhanced scheme.

Table 1: Evaluation Criteria

Criteria
EC-1: User anonymity untraceability
EC-2: Mutual authentication
EC-3: Forward secrecy
EC-4: Session key agreement
EC-5: Resistance to offline password guessing attack
EC-6: Resistance to replay attack
EC-7: Resistance to insider attack
EC-8: Resistance to forgery attack
EC-9: Resistance to stolen verifier attack
EC-10: Resistance to man-in-the-middle attack
EC-11: Resistance to stolen smart card attack
EC-12: Resistance to modification attack
EC-13: Resistance to known session-specific temporary information attack
EC-14: Resistance to known session key attack
EC-15: Local password verification

1.2. Evaluation criteria

To assess the robustness of existing schemes we require an evaluation criterion. Many such evaluation metrics have been proposed[21, 22, 23]. However, Madhusudhan and Mittal[24] in 2012 claimed that the earlier recommended metrics were ambiguous. They then proposed a new set of evaluation criterion. Later, in 2016 Wang et al.[25, 26] refined the metrics presented by Madhusudhan and Mittal and suggested a new set of security requirements and desirable attributes. In this paper we evaluate the robustness of our scheme against the security metrics suggested by Wang et al. and [27] as listed in the Table 1.

1.3. Adversary model

In this paper, we regard the adversarial model as discussed in [25]. Note that the following assumptions about an adversary $\mathcal{A}$'s prowess are quite reasonable and have also been made in recent works[28, 29].

1. $\mathcal{A}$ has the ability to intercept the transmitted messages[30].
2. $\mathcal{A}$ can extract the security parameters stored in the smart card using power analysis technique[31, 32].
3. $\mathcal{A}$ can enumerate the password dictionary offline[33].

1.4. Road map of the paper

The rest of the paper is organized as follows. In Section 2, we briefly introduce the discrete logarithm problem, the one-way hash function, and the DiffieHellman problem; these mathematical concepts form the basis of the security of our proposed scheme. In Section 3, we review Lee et al.'s scheme. Section 4 describes the weakness of Lee et al.'s scheme. Our proposed scheme and corresponding scheme analysis are presented in Sections 5 and 6, respectively. The performance analysis and security requirement comparisons are presented in Section 7. We lastly present our conclusions in Section 8.

2. Preliminaries

In this section, we provide brief introduction to the discrete logarithm problem [34], the one-way hash function (e.g., MD5 [35] or SHA-1 [36], and the Diffie-Hellman problem [37]; these mathematical concepts form the basis of the security of our proposed scheme.

2.1. Discrete logarithm problem and Diffie-Hellman problem

Until now, the discrete logarithm problem has been intractable. Detailed information about the discrete logarithm problem can be found in [34], and we briefly introduce the discrete logarithm problem in the following text. Assume that g is a generator of Z_p^* and that p is a large prime number. Consider the following equation:

$$X = g^x mod\, p \tag{1}$$

If we know g, x and p, computing the modular exponentiation $X = g^x mod\, p$ is trivial. However, if we know g, X, and p, it is computationally infeasible to find x due to the factoring of prime numbers [38]. The problem of solving equation (1) for x is called the discrete logarithm problem. Furthermore, given g, p, $X = g^x mod\, p$, and $Y = g^y mod\, p$, the computation of $K = g^{xy} mod\, p$ is termed the Diffie-Hellman problem [37].

2.2. One-way hash function

A one-way hash function $h : x \rightarrow y$ is a function with the following properties:

- The function h takes message of variable length as the input and converts it into the output of a fixed-length message digest.
- The function h is one-way in the sense that, given x, it is trivial to compute $h(x) = y$. However, given y, it is difficult to compute $h^{-1}(y)= x$.

3. Review of Lee et al.'s scheme

In this section, we review Lee et al.'s authentication scheme [19]. It comprises of three phases: registration phase, login phase, and authentication phase. The detailed steps of the scheme are revealed as follows. Table 2 summarize the notations used in this paper.

Table 2: Notations

Notations	**Description**
U_i	i^{th} mobile user
PW_i	Password of U_i
ID_i	Identity of U_i
S	Medical server
A	Adversary
SC	Smart card
d	Secret key of S
SK	Session Key
p, q	Prime numbers
T_u, T_s	Present time stamp of U_i and S
ΔT	Permissible transmission delay
$h(\cdot)$	Cryptographic one-way hash function
$\|\|$	Concatenation
$\otimes$	Bitwise NOR operation
$\oplus$	Bitwise XOR operation

3.1. Registration phase

1. Suppose a new user U_i wants to register to access the medical server S. U_i selects his/her identity ID_i and password PW_i. U_i sends his registration request $\{ID_i, PW_i\}$ to S via a secure channel.

2. S verifies the validity of the user ID_i, and then computes

$$\begin{aligned} v &= h(K \oplus ID_i) \\ s_1 &= h(PW_i||K) \\ s_2 &= h(h(PW_i||s_1) \\ N &= v \oplus s_2 \oplus H \end{aligned}$$

where K is a secret number of S and H is a constant secret key of S.

3. Finally, S stores $\{ID_i,\ h(\cdot),\ N,\ s_1\ \}$ into a medical smart card and issues the card to U_i through the secure channel.

3.2. Login phase

For login, user U_i inserts his/her medical smart card into a smart card reader and then enters his/her ID_i and PW_i. The login and authentication phase is summarized as follows and also in Figure 2. Next, the smart card performs the following steps:

1. Smart card chooses a random number r_1, and then computes $s_2 = h(h(PW_i||s_1))$ and $C_1 = r_1 \oplus s_2$.
2. Then, the smart card sends login request message $\{\ N,\ ID_i,\ C_1\ \}$ to medical server S via a public channel.

3.3. Authentication phase

1. When S receives the message $\{\ N,\ ID_i,\ C_1\ \}$, it verifies the format of ID_i. If verification holds, then login request is accepted. Otherwise, the login request is rejected.
2. S computes

$$\begin{aligned} v &= h(K \oplus ID_i) \\ s_2^* &= H \oplus N \oplus v \\ r_1^* &= s_2^* \oplus C_1 = s_2^* \oplus r_1 \oplus s_2 \\ a &= r_2 \oplus h(r_1^*||s_2^*) \\ b &= h(s_2^*||r_2||r_1^*) \end{aligned}$$

where r_2 is a random number chosen by S

3. Then, S sends the message $\{a,\ b\}$ to user U_i.

4. After receiving the reply message $\{a,\ b\}$ from S, U_i computes $r_2^* = a \oplus h(r_1||s_2)$. Then, it verifies if $b \stackrel{?}{=} h(s_2||r_2^*||r_1)$. If verification holds, U_i confirms that S is valid. Otherwise, the reply message is rejected.
5. U_i computes $C_2 = h(r_2^*||s_2) \oplus h(PW_i||s_1)$ and sends $\{C_2\}$ to medical server S.
6. After receiving C_2 from U_i, S computes

$$\begin{aligned} u &= h(r_2||s_2^*) \oplus C_2 \\ &= h(r_2||s_2^*) \oplus h(r_2^*||s_2) \oplus h(PW_i||s_1) \\ &= h(PW_i||s_1) \end{aligned}$$

7. Then, S Verifies $s_2^* \stackrel{?}{=} h(u)$. If verification holds, S confirms that U_i is valid. Otherwise, the login request is rejected.
8. Finally, S and U_i can generate a common session key $sk = h(r_1^*||r_2) = h(r_1||r_2^*)$ used for later secure transmission.

3.4. Password change phase

Any legal user U_i can change the password by using the following steps.

1. User U_i inserts his/her medical smart card into a smart card reader and then enters his/her ID_i, PW_i and PW_{new}. Then, smart card sends password change request with the parameters $\{ID_i,\ PW_i,\ PW_{new}\}$ to S.
2. S computes $v = h(K \oplus ID_i)$, $s_1^* = h(PW_{new}||K)$, $s_2^* = h(h(PW_{new}||s_1^*))$ and $N^* = v \oplus s_2^* \oplus H$. Then, S sends $\{s_1^*,\ N^*\}$ to U_i through the secure channel.
3. At last, U_i updates his/her medical smart card with new parameters $\{ID_i,\ h(\cdot),\ s_1^*,\ N^*\}$.

4. Cryptanalysis of Lee et al.'s scheme

In this section, we focus on security loopholes of Lee et al.'s scheme [19]. Before analyzing Lee et al.'s scheme, we make the following three assumptions regarding capability of an adversary A as suggested by Xu et al. [39], Kocher et al. [40], Messerges et al. [41] and Ding et al. [42] respectively. Note that these three assumptions, which are also made in the most recent works [43, 39, 44, 45, 46, 47, 48, 42, 49, 50, 51], are quite reasonable.

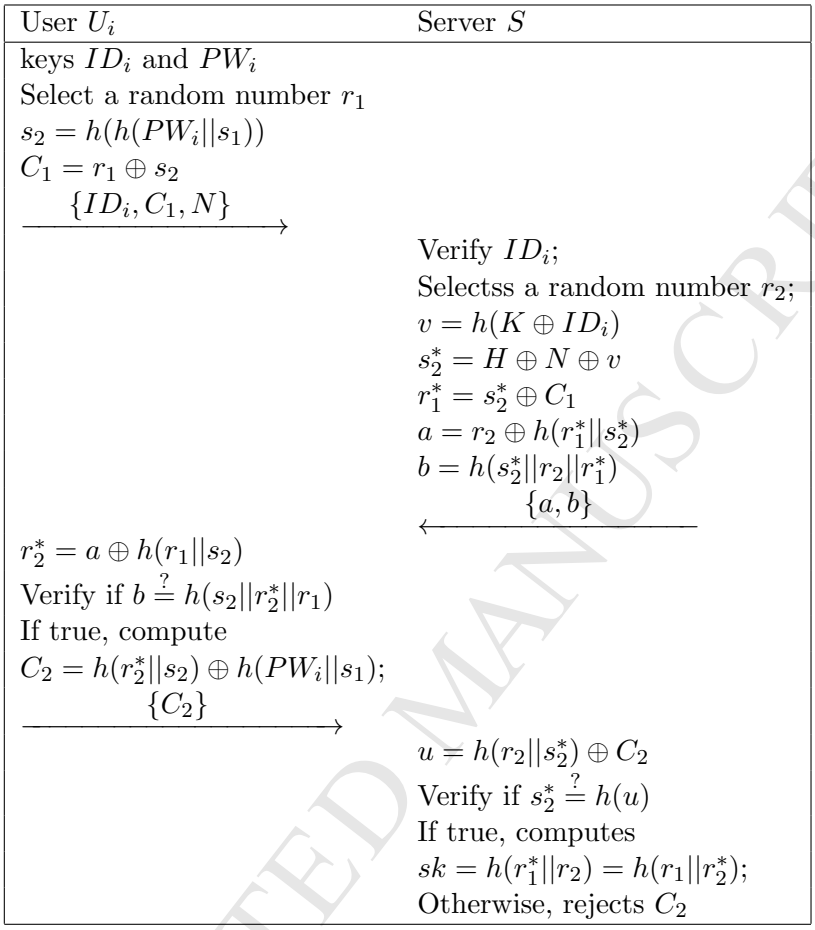


Figure 2: Login and authentication phase of Lee et al. scheme[19].

1. The adversary A has total control over the communication channel between the users and the remote server. That is, A may eavesdrop, block, insert, delete, modify, or intercept any messages transmitted in the channel [39].
2. The adversary A may either steal a user's smart card or picking up the users smart card and then extract the secret values stored in the smart card by side-channel attack techniques [40, 41, 42].
3. The adversary A can off-line enumerate the password dictionary[42].

Following above mentioned assumptions, in the subsequent discussions of the security weakness of the scheme of Lee et al., we assume that an adversary

A can extract the security parameters $\{ID_i, h(\cdot), N, s_1\}$ stored in the legal user's smart card and that the adversary A can also intercept the messages $\{ID_i, C_1, N\}$ and $\{a, b\}$ sent out by the user U_i and the reply message $\{C_2\}$ sent out by the server S. Now, we show various security loopholes existing in Lee et al.'s scheme:

4.1. Vulnerable to offline password guessing attack

In password authentication schemes where the user is permitted to choose his/her password, the user tends to choose a password that can be easily remembered for his/her convenience. However, these easy-to-remember passwords are potentially vulnerable to password guessing attack, in which an adversary can try to guess the users password and then verify his guess. Password guessing attacks include online and offline password guessing attacks. Online password guessing attacks can easily be thwarted by limiting the number of failed logins and limiting the number of continuous login attempts that can occur within a short time interval. However, in off-line password guessing attack, the adversary A intercepts some password related messages transmitted between the user and the server, and then iteratively guesses the user's password and verifies whether his/her guess is correct or not in an offline manner.

Now, let us see how this attack could be successfully launched with the Lee et al.'s scheme. Suppose the user's smart card is lost, an adversary A can reveal all the data $\{ID_i, h(\cdot), N, s_1\}$ under Assumption 2. With the previously intercepted informations $\{ID_i, C_1, N, a, b, C_2\}$ from the public channel, A can obtain U_i's password PW_i as follows:

1. Guesses the value of PW_a to be PW_i.
2. Computes
$$s_2^{'} = h(h(PW_a||s_1))$$
$$r_1^{'} = C_1 \oplus s_2^{'}$$
$$r_2^{'} = a \oplus h(r_1^{'}||s_2^{'})$$
$$b^{'} = h(s_2^{'}||r_2^{'}||r_1^{'})$$
3. Verifies the correctness of PW_a by checking if $b^{'} \stackrel{?}{=} b$.
4. If the verification succeeds, consider PW_a as the user's password. Otherwise adversary A repeats the steps 1-3 until the exact password PW_i is found.

Let $|D_{PW}|$ represent the number of passwords in password dictionary D_{PW}. The running time of the above pointed out attack process is $O(|D_{PW}| \times (4T_{hash} + 2T_{xor}))$, where T_{hash} is the running time for a hash function, T_{xor} is the running time for a XOR operation, respectively. According to Ding et al.'s [43] claim, it is easy to see that, the time for A to recover U_i's password is a linear function of the number of passwords in the password dictionary D_{PW}. In practice, the password dictionary D_{PW} is very limited in nature, for example $|D_{PW}| \leq 10^6$ [52, 53]. Hence the above attack can be done in polynomial time.

4.2. Absence of user anonymity

A protocol with user anonymity protects an individual's sensitive personal information from being acquired by an adversary A through analysing the login information, the resources, or the services being accessed. Moreover, anonymity makes remote user authentication mechanism more strong as an adversary A could not track which users are interacting with the medical server. A simple way to preserve anonymity is to hide user's valid identity during communication. However, in Lee et al.'s scheme, in each login request, user's identity is transmitted in plaintext through login request message $\{ID_i, C_1, N\}$. Moreover, an adversary A can extract the security parameters $\{ID_i, h(\cdot), N, s_1\}$ stored in the legal user's smart card under Assumption 2 and discover the user's identity ID_i. Therefore, anyone can know about the logging user by observing the login request message and user's privacy is not maintained by the scheme. Consequently, an adversary A can misuse the readily available identity of user to break the security walls of the scheme. Therefore, Lee et al.'s scheme fails to preserve user anonymity.

4.3. Vulnerable to user impersonation attack(Spoofing attack)

An adversary A can impersonate a legal user by successfully logging in to the server as follows:

1. A can extract all the data $\{ID_i, h(\cdot), N, s_1\}$ from user's smart card under Assumption 2.
2. A achieves user's password PW_i as discussed in Section 4.1.
3. A achieves user's identity ID_i as discussed in Section 4.2.
4. A chooses a random number r_1 and computes the following values:

$$s_2 = h(h(PW_i||s_1))$$
$$C_1 = r_1 \oplus s_2$$

Then, A sends login request message $\{ N, ID_i, C_1 \}$ to medical server S.

5. When S receives the message $\{ N, ID_i, C_1 \}$, it verifies the format of ID_i. The condition holds as A uses registered user's identity.

$$\begin{aligned} v &= h(K \oplus ID_i) \\ s_2^* &= H \oplus N \oplus v \\ r_1^* &= s_2^* \oplus C_1 = s_2^* \oplus r_1 \oplus s_2 \\ a &= r_2 \oplus h(r_1^* || s_2^*) \\ b &= h(s_2^* || r_2 || r_1^*) \end{aligned}$$

   where r_2 is a random number chosen by S
6. Then, S sends the message $\{a, b\}$ to user U_i.
7. A intercepts the message $\{a, b\}$ and computes $r_2^* = a \oplus h(r_1||s_2)$. Then, it verifies if $b \stackrel{?}{=} h(s_2||r_2^*||r_1)$. The verification hold as $s_2^* = H \oplus N \oplus v = H \oplus v \oplus s_2 \oplus H \oplus v = s_2$.
8. A computes $C_2 = h(r_2^*||s_2) \oplus h(PW_i||s_1)$ and sends $\{C_2\}$ to medical server S
9. After receiving C_2 from U_i, S computes

$$\begin{aligned} u &= h(r_2||s_2^*) \oplus C_2 \\ &= h(r_2||s_2^*) \oplus h(r_2^*||s_2) \oplus h(PW_i||s_1) \\ &= h(PW_i||s_1) \end{aligned}$$

10. Then, S Verifies $s_2^* \stackrel{?}{=} h(u)$. The verification hold as $C_2 = h(r_2^*||s_2) \oplus h(PW_i||s_1)$ and $s_2 = h(PW_i||s_1)$
11. Since, the verification holds, an adversary A is authenticated by S. At last, A and S can generate a common session key $sk = h(r_1^*||r_2) = h(r_1||r_2^*)$.

The above discussion shows that an adversary A can impersonate a legal user by successfully logging in to the medical server S.

4.4. Insider attack

When a user submits his password in its original form to the server, a malicious insider can know the user's password. During the registration phase of Lee et al.s scheme, the user U_i submits plaintext password PW_i

and identity ID_i to the medical server S. This assists direct access of user's password to the privileged insider of the system at S. Having user's password, the insider can impersonate any legal user of the system at other servers where the user employs the same password for his handiness. If the insider turns to become aggressive, he may be dangerous to user's privacy and security of the Lee et al.'s scheme. Therefore, Lee et al.'s scheme cannot withstand insider attack.

4.5. Lacks proper mutual authentication

A good password authentication scheme achieves mutual authentication, meaning that, not only can the server verify the legitimacy of user, but the user can also verify the legitimacy of server. Moreover, no illegal users or servers can impersonate the legal user or the legal server. In Lee et al.'s scheme, mutual authentication is realised. However, the situation of impersonating the user is omitted. As shown in Section 4.3, an adversary A can impersonate a legal user during the login phase. This breaks the mutual authentication setup of the scheme and hence proper mutual authentication is not achieved.

4.6. Denial of service attack

Once A guesses the exact password PW_i and traces the corresponding ID_i of U_i as described in Sections 4.1 and 4.2 respectively, he can change the password of U_i as follows

1. A inserts the stolen/found smart card into the card reader, keys ID_i, PW_i and PW_{new} of U_i. Then, smart card sends password change request with parameters $\{ID_i, PW_i, PW_{new}\}$ to S.
2. S computes $v = h(K \oplus ID_i)$, $s_1^* = h(PW_{new}||K)$, $s_2^* = h(h(PW_{new}||s_1^*))$ and $N^* = v \oplus s_2^* \oplus H$. Then, S sends $\{s_1^*, N^*\}$ to U_i.
3. At last, smart card is updated with new parameters $\{ID_i, h(\cdot), s_1^*, N^*\}$. Now the new password is successfully updated. Now A replaces the smart card of U_i. Afterward, the registered legal user U_i cannot make any valid login requests since his/her old password will not work anymore.

The above discussion shows that Lee et al.'s scheme cannot withstand Denial of service attack.

4.7. Wrong password cannot be quickly detected-Local password verification

In the login phase of Lee et al.'s scheme, the user U_i inputs his/her identity ID_i and password PW_i; however the smart card does not verify the legality of user's password PW_i. Therefore, even if the user U_i incorrectly inputs his/her password PW_i, Step 1-4 of authentication phase are still performed. It shows the inefficiency of scheme in incorrect input detection. This leads to unnecessarily extra communication and computational overheads during the login and authentication phases.

5. The Proposed Scheme

The proposed scheme consists of the following phases.

5.1. Initialization

Server S selects two large prime integers (p, q) and computes $n = p \times q$ and $\phi(n) = (p-1) \times (q-1)$. Then, S selects an integer e such that $gcd(e, \phi(n)) = 1$ and $1 < e < \phi(n)$. It computes an integer d such that $d \equiv e^{-1} mod\ \phi(n)$. Lastly, e and n are made public while (p, q) and d are kept secret by the server S.

5.2. Registration Phase

This phase consists of the following steps:

1. User U_i freely selects his or her password PW_i, identity ID_i and a random number r and sends $\{h(PW_i||r),\ ID_i\}$ to S via a secure communication channel.
2. S generates a random number b and computes

$$\begin{aligned} x &= b^e\ mod\ n, \\ A_u &= h(d||b) \oplus h(ID_i), \\ B_u &= h(d||ID_i) \oplus h(PW_i||r), \end{aligned}$$

   where d is the S's secret key. Lastly, S stores $\{A_u,\ B_u,\ x,\ e,\ n,\ h(\cdot)\}$ in smart card and sends it to U_i via a secure channel.
3. U_i computes $C_u = h(ID_i||PW_i) \oplus r$ and $C_t = h(ID_i \otimes PW_i \otimes r)$ and injects $\{C_u,\ C_t\}$ into smart card. Finally, the smart card contains $\{A_u,\ B_u,\ C_u,\ C_t,\ x,\ e,\ n,\ h(\cdot)\}$.

The registration phase is summarized in Figure 3.

User U_i	Server S
Selects ID_i, PW_i.	
$h(PW_i\|\|r)$.	
$\xrightarrow{\{h(PW_i\|\|r), ID_i\}}$	
(via secure channel)	Generates a random number b.
	$x = b^e \, mod \, n$.
	$A_u = h(d\|\|b) \oplus h(ID_i)$.
	$B_u = h(d\|\|ID_i) \oplus h(PW_i\|\|r)$.
	Stores $\{A_u, B_u, x, e, n, h(\cdot)\}$ in SC.
	$\xleftarrow{\{Smart \;\; card\}}$
	(via secure channel)
$C_u = h(ID_i\|\|PW_i) \oplus r$.	
$C_t = h(ID_i \otimes PW_i \otimes r)$.	
Injects $\{C_u, C_t\}$ into SC.	

Figure 3: Registration phase.

5.3. Login and authentication phase

The detailed steps of login and authentication phases is as follows and also in Figure 4:

1. $U_i \rightarrow S : M_1 = \{z, V_2, V_3, V_5, T_u\}$
   U_i inserts his or her smart card into the card reader device and enters password PW_i and identity ID_i. Then, the device computes $r = C_u \oplus h(ID_i||PW_i)$ and verifies $ID_i \otimes PW_i \otimes r \stackrel{?}{=} C_t$. If the verification holds, then it selects a random number N_u and computes the following values; Otherwise, it terminates the login process.

$$\begin{aligned} V_1 &= A_u \oplus h(ID_i), \\ V_2 &= V_1 \oplus N_u, \\ V_3 &= h(V_1||N_u) \oplus ID_i, \\ V_4 &= B_u \oplus h(PW_i||r), \\ V_5 &= h(V_2||V_3||V_4||T_u), \\ z &= x \oplus T_u. \end{aligned}$$

   where T_u is the present timestamp of U_i. Then, U_i sends $M_1 = \{z, V_2, V_3, V_5, T_u\}$ to S.

2. $S \rightarrow U_i$: M_2=$\{V_6, W, T_s^{'}\}$
When M_1 is received, S checks the recentness of T_u using $T_s - T_u \leq \Delta T$, where T_s is the present timestamp of S and ΔT is the allowed time interval for the communication delay between U_i and S. If it does not hold, S rejects M_1. Otherwise, S finds $x = z \oplus T_u$. Next, S decrypts $x^d \, mod \, n$ to find b. Further, S computes

$$\begin{aligned} N_u^* &= V_2 \oplus h(d||b), \\ ID_i^* &= V_3 \oplus h(h(d||b)||N_u^*), \\ V_4^* &= h(d||ID_i^*), \\ V_5^* &= h(V_2||V_3||V_4^*||T_u). \end{aligned}$$

S then verifies $V_5^* \stackrel{?}{=} V_5$. If the verification holds, U_i is authenticated by S. Otherwise, S rejects M_1. Once U_i is authenticated, S generates a random number r_s and computes

$$\begin{aligned} SK_s &= h(V_4^*||N_u^*||r_s), \\ V_6 &= r_s \oplus h(N_u^* \oplus V_4^*), \\ W &= h(SK_s||N_u^*||r_s||T_s), \end{aligned}$$

and sends reply message M_2=$\{V_6, W, T_s\}$ to U_i.

3. When M_2 is received, U_i checks the recentness of T_s using $T_u^{'} - T_s \leq \Delta T$, where $T_u^{'}$ is the present timestamp of U_i. If it does not hold, U_i rejects M_2. Otherwise, U_i computes the session key as follows:

$$\begin{aligned} r_s^* &= V_6 \oplus h(N_u \oplus V_4), \\ SK_u &= h(V_4||N_u||r_s^*), \\ W^* &= h(SK_u||N_u||r_s^*||T_s). \end{aligned}$$

U_i then verifies $W^* \stackrel{?}{=} W$. If the verification fails, U_i rejects M_2. Otherwise, U_i authenticates S. The above verification ensures the successful mutual authentication between U_i and S. Hence, both U_i and S agree upon a common secret session key $SK_u = h(V_4||N_u||r_s) = SK_s$.

5.4. Password change phase

U_i inserts his/her smart card into the card reader device and enters password PW_i, identity ID_i and new password PW_i^{new}. Then, the device computes $r = C_u \oplus h(ID_i||PW_i)$ and verifies $h(ID_i \otimes PW_i \otimes r) \stackrel{?}{=} C_t$. If verification

User U_i	Server S
Inputs ID_i, PW_i. Computes $r = C_u \oplus h(ID_i \| \| PW_i)$. Verifies $h(ID_i \otimes PW_i \otimes r) \stackrel{?}{=} C_t$ If true, selects N_u and computes $V_1 = A_u \oplus h(ID_i)$, $V_2 = V_1 \oplus N_u$, $V_3 = h(V_1 \| \| N_u) \oplus ID_i$, $V_4 = B_u \oplus h(PW_i \| \| r)$, $V_5 = h(V_2 \| \| V_3 \| \| V_4 \| \| T_u)$, $z = x \oplus T_u$. $M_1 = \{z, V_2, V_3, V_5, T_u\} \longrightarrow$	
	Checks validity of T_u using $T_s - T_u \leq \Delta T$. If so, obtains $x = z \oplus T_u$ and $b = x^d \, mod \, n$. $N_u^* = V_2 \oplus h(d \| \| b)$, $ID_i^* = V_3 \oplus h(h(d \| \| b) \| \| N_u^*)$, $V_4^* = h(d \| \| ID_i^*)$, $V_5^* = h(V_2 \| \| V_3 \| \| V_4^* \| \| T_u)$. Verifies $V_5^* \stackrel{?}{=} V_5$. If true, S authenticates U_i. Generates r_s. Computes $SK_s = h(V_4^* \| \| N_u^* \| \| r_s)$, $V_6 = r_s \oplus h(N_u^* \oplus V_4^*)$, $W = h(SK_s \| \| N_u^* \| \| r_s \| \| T_s)$, $M_2 = \{V_6, W, T_s\} \longleftarrow$
Checks validity T_s using $T_u^{'} - T_s \leq \Delta T$. Computes $r_s^* = V_6 \oplus h(N_u \oplus V_4)$, $SK_u = h(V_4 \| \| N_u \| \| r_s^*)$, $W^* = h(SK_u \| \| N_u \| \| r_s^* \| \| T_s)$. Verifies $W^* \stackrel{?}{=} W$. If true, U_i authenticates S	
Shared session key is $SK_u = h(V_4 \| \| N_u \| \| r_s) = SK_s$.	

Figure 4: Login and authentication phase.

fails, it rejects the request. Otherwise, the following values are computed:

$$\begin{aligned} B_u^{'} &= B_u \oplus h(PW_i||r) \oplus h(PW_i^{new}||r) \\ &= h(d||ID_i) \oplus h(PW_i^{new}||r), \\ C_u^{'} &= h(ID_i||PW_i^{new}) \oplus r, \\ C_t^{'} &= h(ID_i \otimes PW_i^{new} \otimes r). \end{aligned}$$

Finally, the values C_u, B_u and C_t are substituted with $C_u^{'}$, $B_u^{'}$ and $C_t^{'}$, respectively.

6. Security Analysis

In this section, we show that our scheme is provably secure against an attacker for deriving the private key d of the server S, the identity ID_i of a legal user U_i and the session key SK between U_i and S.

6.1. Formal Security Analysis

We utilize the formal definitions of the one-way hash function $h(\cdot)$ and integer factorization problem (IFP) defined in Definitions 1 and 2, respectively.

Definition 1. *A collision-resistant one-way hash function $h : \{0,1\}^* \rightarrow \{0,1\}^l$ is a deterministic algorithm which on input arbitrary length binary string $x \in \{0,1\}^*$ outputs a fixed-length l-bit binary string $h(x) \in \{0,1\}^l$ [54]. If $Adv_{\mathcal{A}}^{HASH}(t)$ is an attacker $\mathcal{A}$'s advantage in finding collision, then it is defined by*

$$\begin{aligned} Adv_{\mathcal{A}}^{HASH}(t) \;=\; & Pr[(x,y) \in_R \mathcal{A} : x \neq y \\ & \text{and } h(x) = h(y)], \end{aligned}$$

where $Pr[X]$ denotes the probability of an event X in a random experiment, and $(x,y) \in_R \mathcal{A}$ is a pair randomly selected by $\mathcal{A}$. $\mathcal{A}$ is also allowed to be probabilistic and the probability in the advantage is computed over the random choices made by $\mathcal{A}$ with the execution time t. $h(\cdot)$ is called collision-resistant if $Adv_{\mathcal{A}}^{HASH}(t) \leq \epsilon_1$, for any sufficiently small $\epsilon_1 > 0$.

Definition 2. *Let Gen_F be a polynomial-time algorithm that on input 1^ρ, output (n,p,q), where $n = pq$, and p and q be ρ-bit distinct primes. The factoring assumption relative to Gen_F states that given N, it is computationally*

infeasible to derive the prime factors p and q, except with a negligible probability in ρ. This problem is formally defined as follows [55].

For any probabilistic polynomial-time (PPT) $\mathcal{A}$, its factoring advantage is given by

$$Adv^{IFP}_{Gen_F,\mathcal{A}}(\rho) = Pr[(n,p,q) \leftarrow Gen_F(1^\rho) : \mathcal{A}(n) = \{p,q\}].$$

The factoring assumption (with respect to Gen_F) states that $Adv^{IFP}_{Gen_F,\mathcal{A}}(\rho)$ is negligible in ρ for every PPT $\mathcal{A}$. $(t_{IFP}, \epsilon_{IFP})$-IFP assumption holds if $Adv^{IFP}_{Gen_F,\mathcal{A}}(\rho) \leq \epsilon_{IFP}(\rho)$, for any sufficiently small $\epsilon_{IFP}(\rho) > 0$, and its running time is at most t_{IFP}.

We apply the method of contradiction proof in our formal security analysis as presented in [56], [57], [58], [59], [60], [61], [62], [63]. For this purpose, we assume that the following two random oracles are available to the attacker $\mathcal{A}$:

- $HashOracle$: It will output the input string x from the corresponding hash value $y = h(x)$.
- $IFPOracle$: It will output the private key d of the server S from the public values $n = p \times q$ and e, where $ed \equiv 1 \pmod{(p-1)(q-1)}$.

Theorem 1. *Under the assumption that the one-way hash function $h(\cdot)$ closely behaves like a random oracle, the proposed scheme is provably secure against an attacker for deriving the private key d of the server S, the identity ID_i of a legal user U_i and the session key SK between U_i and S, if IFP is intractable.*

Proof. In this proof, we construct an attacker $\mathcal{A}$ who will have the ability to derive the private key d of the server S, the identity ID_i of a legal user U_i and the session key SK between U_i and S by intercepting the messages during the login and authentication phase. With the access to both $HashOracle$ and $IFPOracle$ oracles, $\mathcal{A}$ can run the experiment for the proposed user authentication scheme, say UAS, which is given in Algorithm 1.

The success probability for the experiment $EXP^{HASH,IFP}_{\mathcal{A},UAS}$ is given by $Succ_{\mathcal{A}} = |2Pr[EXP^{HASH,IFP}_{\mathcal{A},UAS} = 1] - 1|$ and the advantage of this experiment becomes $Adv_{\mathcal{A}}(t, q_{Hash}, q_{IFP}) = \max_{\mathcal{A}}\{Succ_{\mathcal{A}}\}$, where the maximum is taken

Algorithm 1 $EXP_{\mathcal{A},UAS}^{HASH,IFP}$

1: Eavesdrop the login message $M_1 = \langle z,\ V_2,\ V_3, V_5, T_u \rangle$ during the login and authentication phase, where $x = b^e \pmod{n}$.
2: Call $IFPOracle$ oracle on input $n = p \times q$ and the public key e of the server S to derive the private key d of S as $d \leftarrow IFPOracle(n, e)$.
3: Call $HashOracle$ oracle on input V_5 to retrieve the information $(V_1'||V_3'||V_4'||T_u') \leftarrow HashOracle(V_5)$.
4: **if** $(T_u' \neq T_u)$ **then**
5: **return** 0 (Failure)
6: **else**
7: Calculate $x = z \oplus T_u$. Using d, decrypt x to retrieve the secret random number b of S as $b^* = x^d \pmod{n}$.
8: Using V_2, d and b^*, calculate $N_u^* = V_2 \oplus h(d||b^*)$, $ID_i^* = V_3 \oplus h(h(d||b^*)||N_u^*)$ and $V_4 = h(d||ID_i^*)$.
9: Eavesdrop the authentication message $M_2 = \langle V_6, W, T_s \rangle$ during the login and authentication phase.
10: Calculate $r_s^* = V_6 \oplus h(N_u^* \oplus V_4)$.
11: Calculate $SK = h(V_4||N_u^*||r_s^*)$.
12: Calculate $W^* = h(SK||N_u^*||r_s^*||T_s)$.
13: **if** $(W^* \neq W)$ **then**
14: Accept d, ID_i^* and SK as the correct private key of S, identity of U_i and session key shared between U_i and S, respectively.
15: **return** 1 (Success)
16: **else**
17: **return** 0 (Failure)
18: **end if**
19: **end if**

over all $\mathcal{A}$ with the execution time t, and the number of queries q_{Hash} and q_{IFP} made to $HashOracle$ and $IFPOracle$ oracles, respectively. The proposed scheme is provably secure against the attacker $\mathcal{A}$ for deriving d, ID_i and SK , if $Adv_{\mathcal{A}}(t, q_{Hash}, q_{IFP}) \leq \delta$, for any sufficiently small $\delta > 0$.

Now, according to $EXP_{\mathcal{A},UAS}^{HASH,IFP}$ in Algorithm 1, if $\mathcal{A}$ has the ability to invert one-way hash function $h(\cdot)$, and to solve the IFP to derive $d = e^{-1} \pmod{(p-1)(q-1)}$ using the public key e of S and n, he/she can compute the correct d, ID_i and the session key SK, and also win the game. However, it is computationally hard for $\mathcal{A}$, which is evident from both Def-

initions 1 and 2 that $Adv_{\mathcal{A}}^{HASH}(t) \leq \epsilon_1$ and $Adv_{Gen_F,\mathcal{A}}^{IFP}(\rho) \leq \epsilon_{IFP}(\rho)$. Thus, $Adv_{\mathcal{A}}(t, q_{Hash}, q_{IFP})$ depends on both $Adv_{\mathcal{A}}^{HASH}(t)$ and $Adv_{Gen_F,\mathcal{A}}^{IFP}(\rho)$. As a result, $Adv_{\mathcal{A}}(t, q_{Hash}, q_{IFP}) \leq \delta$. Therefore, the theorem is proved.

6.2. Informal Security Analysis

This section further analyzes that the proposed scheme can protect the following known attacks.

6.2.1. User anonymity

In the proposed scheme, according to Assumption A2, an attacker may steal U_i's smart card and extract the information $\{A_u, B_u, C_u, C_t, x, e, n, h(\cdot)\}$ from the smart card. Here, ID_i is related with parameters A_u, C_u and C_t. However, from these parameters, it is impossible to derive U_i's identity ID_i because ID_i is protected by the secret random values b and r, S's master secret key d and U_i's password PW_i. This shows that the attacker cannot obtain the identity ID_i of U_i without knowing d, r, b and PW_i. Therefore, the improved scheme preserves user anonymity.

6.2.2. Mutual authentication

The proposed scheme ensures the mutual authentication between U_i and S. S authenticates U_i by verifying $V_5^* \stackrel{?}{=} V_5$. A valid V_5 can be computed by legitimate U_i because of V_4^* in V_5^*. As discussed in Section 6.2.1, since an attacker does not know d and ID_i, so valid V_4 and V_5 values cannot be computed by any malicious user. Thus, S authenticates U_i. Also, S can be authenticated by U_i by verifying $W^* \stackrel{?}{=} W$. Therefore, the proposed scheme achieves proper mutual authentication.

6.2.3. Offline password guessing attack

In the proposed scheme, an attacker may steal U_i's smart card. In such a situation, attacker disclose the stored data $\{A_u, B_u, C_u, C_t, x, e, n, h(\cdot)\}$ under Assumption A2. Using intercepted message M_1=$\{z, V_2, V_3, V_5, T_u\}$, attacker may try to obtain U_i's password PW_i. As we illustrated above, throughout the proposed scheme, U_i's password PW_i only makes three presences as B_u, C_u and C_t. Manifestly, the attacker cannot launch an offline password guessing attack without knowing r and ID_i. ID_i and r in plaintext are neither transmitted through any of the messages $\{M_1, M_2\}$ over the communication network nor stored in the U_i's smart card. Moreover, we have proved that the proposed scheme achieves user anonymity in Section 6.2.1.

Therefore, the proposed scheme is resilient to the offline password guessing attack.

6.2.4. Replay attack

A replay attack involves retransmitting earlier intercepted messages. Under Assumption A1, an attacker might intercept $\{M_1, M_2\}$, which are transmitted between S and U_i. However, the timestamp values T_u and T_s are used in the proposed scheme to withstand the replay attack. An attacker may retransmit the intercepted messages without any alteration such as $M_1 = \{z, V_2, V_3, V_5, T_u\}$ in step 1 and M_2=$\{V_6, W, T_s\}$ in step 2. S and U_i can simply identify the attack by verifying the recentness of those timestamps.

By retransmitting the intercepted message M_1 to S with an alteration such as $M_1 = \{z, V_2, V_3, V_5, T_u^*\}$ to S, where T_u^* is the modified timestamp, an attacker may act as a legal U_i. Now, in server side, the verification $T_s - T_u^* \leq \Delta T$ will be true. Then, S computes $z \oplus T_u^*$, but $z \oplus T_u^* = x \oplus T_u \oplus T_u^* \neq x$. So that S cannot finds a random number $b(= x^d mod\ n)$. Without knowing b, S cannot derive an identity (ID_i) and random number N_u of U_i, and cannot compute the parameters V_4 and V_5. Thus, an attacker cannot pass the verification $V_5^* \stackrel{?}{=} V_5$. As this verification fails, the attacker will not be verified as a legal user.

An attacker may retransmit the intercepted message M_2 to U_i with an alteration such as M_2=$\{V_6, W, T_s^*\}$, where T_s^* is the modified timestamp, an attacker may act as a legal S. Now the verification $T_u^{'} - T_s^* \leq \Delta T$ will be true. However, $V_6(= r_s \oplus h(N_u^* \oplus V_4^*))$ and $W(= h(SK_u||N_u||r_s||T_s))$ are computed freshly in every session due to the random numbers r_s and N_u and the timestamp T_s. As well, since the random numbers N_u and r_s are generated freshly in every session, the session key $SK_u = SK_s = h(V_4||N_u||r_s)$ has a new value in every session. Thus, an attacker cannot act as a legal S by retransmitting M_2. Therefore, the proposed scheme successfully withstands the replay attack.

6.2.5. Session key agreement

Subsequent to the authentication process, the U_i and S will establish a session key SK_u. Since the attacker has no knowledge of V_4, N_u and r_s, the session key cannot be directly computed, as it is protected by a one-way hash function. Hence, the proposed scheme ensures the secrecy of future session keys.

6.2.6. Forward secrecy

The forward secrecy means that even though all participant's long term secret keys are compromised, it will not helps to discover of any past session key. Now, in the proposed scheme, if any long term secret of either the user(PW_i) or server(d) or all are compromised, it never supports in recovering any earlier session key(e.g., SK_{i-1}) because there is no significant correlation among SK_{i-1}, SK_i, SK_{i+1}. In particular, there are two random numbers, i.e., N_u and rs, involved in the computation of the session key, i.e., $SK_u = SK_s = h(V_4||N_u||r_s)$, which are conventional to be different each time. Consequently, in the proposed scheme, all the previous session keys will remain secure. Therefore, the proposed scheme achieves forward secrecy.

6.2.7. Man-in-the-middle attack

In the proposed scheme, the Man-in-the-middle attack is prevented by mutual authentication between U_i and S. As a result, Man-in-the-middle attacks are thwarted since we show that the proposed scheme achieves mutual authentication in Section 6.2.2.

6.2.8. Forgery attack

In the proposed scheme, a valid message M_1 can only be generated by a valid U_i. In order to achieve this, the attacker must know r, d and ID_i. However, we proved in Section 6.2.1 that the improved scheme achieves user anonymity, so the attacker cannot retrieve ID_i. Also, ID_i and r are neither transmitted through $\{M_1, M_2\}$ over the communication network nor stored in the smart card. Moreover, we have already proved that the proposed scheme achieves mutual authentication and withstands replay attack in Section 6.2.2 and Section 6.2.4 respectively. Hence, the proposed scheme is resilient to the forgery attack as well.

6.2.9. Insider attack

In the proposed scheme, U_i sends $\{ID_i, h(PW_i||r)\}$ to S in the registration phase of the proposed scheme. As a result, it is impossible for the insider to derive PW_i without knowing r. Moreover, in the password change phase, U_i can update his/her password PW_i without any assistance from S. Since the insider has no chance of obtaining U_i's password, the proposed scheme can resist the insider attack.

6.2.10. Stolen verifier and modification attacks

In the proposed scheme, the S does not store U_i's passwords. S only keeps the secret key d. Therefore, the proposed scheme can withstand the stolen verifier and modification attacks.

6.2.11. Smart card loss Attacks

Suppose U_i loses his/her smart card; an attacker can examine all of the data from the smart card according Assumption A2. The attacker then attempts to derive the password from the examined data. Here, PW_i is related with parameters B_u, C_u and C_t. However, from these parameters, it is impossible to find U_i's password PW_i because PW_i is protected by r and ID_i. In addition, we have already proved that the proposed scheme achieves user anonymity in Section 6.2.1 and the random value r is neither sent through messages M_1 nor stored in the smart card. This shows that the attacker cannot obtain the password PW_i of U_i without knowing r and ID_i. Therefore, the proposed scheme can withstand smart card loss attacks.

6.2.12. Local password verification

In the proposed scheme, before logging into the S, the device verifies the legality of ID_i and PW_i. Therefore, even if the user U_i inputs his/her PW_i or ID_i or both incorrectly by mistake, that will be detected by the verification $C_t \stackrel{?}{=} C_t'$. Thus, the proposed scheme provides a facility for an incorrect input detection. As well, without the knowing ID_i, PW_i and r, the attacker cannot correctly compute C_t' and subsequently, the verification $C_t = C_t'$ fails. Thus, the proposed scheme thwarts illegal access using local password verification.

6.2.13. User-friendliness

In the proposed scheme, U_i can freely choose his/her identity ID_i and password PW_i. Also, the U_i can update the password PW_i easily without the S's help within minimal time since he/she does not have to go through the entire Section 5.3. This shows that the proposed scheme is hassle-free and user-friendly.

7. Performance Analysis

In this section, we compare the security requirements and performance of the proposed scheme with the other related schemes, such as Wei et al. [12], Lee et al. [19], Wu et al. [20], Chaturvedi et al. [64] and Qiu et al. [65] to

manifest the advantages of the proposed scheme. In order to carry out the performance analysis, we used following notations:

- T_h is the computational cost of a hash operation.
- T_{mexp} is the computational cost of a modular exponent operation.
- T_{xor} is the computational cost of a XOR operation
- T_{pm} the time for executing a point multiplication operation.

Since the login and authentication phase is the most important body of an authentication scheme, we mainly focus on this phase. An experiment results of [66] and [67] demonstrate that computation costs(execution time) of T_h, T_{mexp} and T_{pm} are 0.0005, 0.522 and 0.13 seconds. As the computational cost of XOR operation is negligible as compared to other cryptographic operations, we do not consider T_{xor} into account. Table 3 shows the computation cost comparisons of the proposed scheme with the other related schemes and the proposed scheme. Compared with other related schemes of Wei et al., Lee et al., Wu et al. and Chaturvedi et al., the proposed scheme needs very less computational cost. Compared to Qiu et al.'s scheme, the computation cost of the proposed scheme is little increased. This is justified, because the proposed scheme achieves all the security requirements while Qiu et al.'s scheme does not. Hence, the proposed scheme spending very less computational cost to achieve higher security and usability.

Table 3: Computational cost comparison

Schemes	**Participant**		**Total**
	User	**Server**	
Wei et al. [12]	$5T_h + T_{mexp}$	$5T_h + 2T_{mexp}$	$10T_h + 3T_{mexp} \approx 1571ms$
Lee et al. [19]	$T_h + T_{mexp}$	$9T_h + 3T_{mexp}$	$10T_h + 4T_{mexp} \approx 2093ms$
Wu et al. [20]	$3T_h + 3T_{mexp}$	$4T_h + 4T_{mexp}$	$7T_h + 7T_{mexp} \approx 3658ms$
Chaturvedi et al. [64]	$4T_h + T_{mexp}$	$10T_h + T_{mexp}$	$10T_h + 2T_{mexp} \approx 1049ms$
Qiu et al. [65]	$8T_h + 2T_{pm}$	$5T_h + 2T_{pm}$	$13T_h + 4T_{pm} \approx 527ms$
Ours	$8T_h$	$7T_h + T_{mexp}$	$15T_h + 1T_{mexp} \approx 530ms$

Assume that the digest (output) of hash function(for SHA-1 [36]), identity (ID_i), random number is 160 bits and password PW_i are 160-bit long, and timestamp is 32-bit long. In the proposed scheme, the message $M_1 = \{z, V_2, V_3, V_5, T_u\}$ needs (160+160+160+160+32)=672 bits and the message $M_2 = \{V_6, W, T_s\}$ needs $(160 + 160 + 32) = 352$ bits. Therefore, the proposed scheme requires (672+352)=1024 bits for the communication cost of two messages transmitted between U_i and S. Table 4 shows that the communication cost comparisons of the proposed scheme and other related schemes. Compared with related schemes of Wei et al., Chaturvedi et al. and Qiu et al., the proposed scheme needs very less communication cost. Compared to Lee at al.'s scheme, the communication cost of the proposed scheme is little increased. This is justified, because the proposed scheme achieves all the security requirements while Lee et al.'s scheme does not. The communication cost of Wu et al.'s scheme and the proposed scheme is equal(1024 bits) which means that the same number of parameters are transmitted over the public channel to meet the intention of authentication. The security requirement comparison of the proposed scheme and other related schemes is summarized in Table 5, from which we can see that the proposed scheme is more secure and friendly than other related schemes.

Table 4: Communication cost comparison

Schemes	**Communication cost**	
	Number of messages	**Number of bits**
Wei et al. [12]	3	1824
Lee [19]	2	864
Wu et al. [20]	2	1024
Chaturvedi et al. [64]	2	1280
Qiu et al. [65]	3	1504
Ours	2	1024

8. Conclusion

We have analyzed the Lee et al.'s scheme and proved that their scheme does not achieve user anonymity and mutual authentication. In addition, it

Table 5: Security requirements comparison

Security requirements	**Schemes**					
	Wei et al. [12]	**Lee [19]**	**Wu et al. [20]**	**Chaturvedi et al. [64]**	**Qiu et al. [65]**	**Ours**
User anonymity	$\times^{[65]}$	$\times^{*}$	$\times^{[19]}$	✓	✓	✓
Mutual authentication	$\times^{[65]}$	$\times^{*}$	$\times^{[19]}$	✓	✓	✓
Forward secrecy	✓	✓	✓	✓	✓	✓
Session key agreement	✓	✓	✓	✓	✓	✓
Local password verification	✓	$\times^{*}$	✓	✓	✓	✓
Offline password guessing attack	$\times^{[65]}$	$\times^{*}$	$\times^{[19]}$	✓	✓	✓
Replay attack	$\times^{[65]}$	✓	✓	$\times^{[68]}$	✓	✓
Man-in-the middle attack	$\times^{[65]}$	✓	✓	$\times^{[68]}$	✓	✓
Stolen verifier attack	✓	✓	✓	$\times^{[68]}$	✓	✓
Modification attack	✓	✓	✓	✓	✓	✓
Forgery attack	$\times^{[65]}$	$\times^{*}$	$\times^{[19]}$	$\times^{[68]}$	✓	✓
Insider attack	✓	✓	$\times^{[19]}$	$\times^{[68]}$	$\times^{*}$	✓
Smart card loss attack	✓	✓	✓	✓	✓	✓
User-friendliness	✓	$\times^{*}$	✓	✓	✓	✓

Note: ✓ : achieved; $\times$: not achieved; $*$: we have shown.

is defenseless against off-line password guessing, insider, user impersonation and Denial of Service (DoS) attacks. In order to fix the weaknesses of the Lee et al.'s scheme, we have proposed a more secure authentication scheme with key agreement. Performance evaluation and security analysis shows that the proposed scheme is invulnerable to various attacks, and it is also suitable for safe and secure communications.

Acknowledgments

We would like to thank the anonymous reviewers for their positive suggestions and comments that highly improve the readability and completeness of the paper. Also we would like to acknowledge the management of VIT University for providing the wonderful support to do the research work.

References

[1] P. B. Elberg, Electronic patient records and innovation in health care services, International journal of medical informatics 64 (2) (2001) 201–205.

[2] F. Leiner, W. Gaus, R. Haux, P. Knaup-Gregori, Thesaurus of medical documentation, Medical Data Management: A Practical Guide (2003) 137–195.

[3] C. Lovis, R. H. Baud, J.-R. Scherrer, Internet integrated in the daily medical practice within an electronic patient record, Computers in biology and medicine 28 (5) (1998) 567–579.

[4] A. Van't Riet, M. Berg, F. Hiddema, K. Sol, Meeting patients' needs with patient information systems: potential benefits of qualitative research methods, International journal of medical informatics 64 (1) (2001) 1–14.

[5] C. Lambrinoudakis, S. Gritzalis, Managing medical and insurance information through a smart-card-based information system, Journal of Medical Systems 24 (4) (2000) 213–234.

[6] Z.-Y. Wu, Y.-C. Lee, F. Lai, H.-C. Lee, Y. Chung, A secure authentication scheme for telecare medicine information systems, Journal of medical systems 36 (3) (2012) 1529–1535.

[7] L. Dunlop, Electronic health records: Interoperability challenges patients' right to privacy, Shidler JL Com. & Tech. 3 (2006) 1.

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

[9] T. Cao, J. Zhai, Improved dynamic id-based authentication scheme for telecare medical information systems, Journal of medical systems 37 (2) (2013) 9912.

[10] Z.-Y. Wu, Y.-C. Lee, F. Lai, H.-C. Lee, Y. Chung, A secure authentication scheme for telecare medicine information systems, Journal of medical systems 36 (3) (2012) 1529–1535.

[11] H. Debiao, C. Jianhua, Z. Rui, A more secure authentication scheme for telecare medicine information systems, Journal of Medical Systems 36 (3) (2012) 1989–1995.

[12] J. Wei, X. Hu, W. Liu, An improved authentication scheme for telecare medicine information systems, Journal of medical systems 36 (6) (2012) 3597–3604.

[13] Z. Zhu, An efficient authentication scheme for telecare medicine information systems, Journal of medical systems 36 (6) (2012) 3833–3838.

[14] T.-F. Lee, An efficient chaotic maps-based authentication and key agreement scheme using smartcards for telecare medicine information systems, Journal of medical systems 37 (6) (2013) 9985.

[15] Q. Jiang, J. Ma, Z. Ma, G. Li, A privacy enhanced authentication scheme for telecare medical information systems, Journal of medical systems 37 (1) (2013) 1–8.

[16] T. Cao, J. Zhai, Improved dynamic id-based authentication scheme for telecare medical information systems, Journal of medical systems 37 (2) (2013) 9912.

[17] Q. Xie, J. Zhang, N. Dong, Robust anonymous authentication scheme for telecare medical information systems, Journal of medical systems 37 (2) (2013) 9911.

[18] M. K. Khan, S.-K. Kim, K. Alghathbar, Cryptanalysis and security enhancement of a 'more efficient & secure dynamic id-based remote user authentication scheme', Computer Communications 34 (3) (2011) 305–309.

[19] T.-F. Lee, I.-P. Chang, T.-H. Lin, C.-C. Wang, A secure and efficient password-based user authentication scheme using smart cards for the integrated epr information system, Journal of medical systems 37 (3) (2013) 9941.

[20] Z.-Y. Wu, Y. Chung, F. Lai, T.-S. Chen, A password-based user authentication scheme for the integrated epr information system, Journal of medical systems 36 (2) (2012) 631–638.

[21] I.-E. Liao, C.-C. Lee, M.-S. Hwang, A password authentication scheme over insecure networks, Journal of Computer and System Sciences 72 (4) (2006) 727–740.

[22] S. Wu, Y. Zhu, Q. Pu, Robust smart-cards-based user authentication scheme with user anonymity, Security and Communication Networks 5 (2) (2012) 236–248.

[23] G. Yang, D. S. Wong, H. Wang, X. Deng, Two-factor mutual authentication based on smart cards and passwords, Journal of Computer and System Sciences 74 (7) (2008) 1160–1172.

[24] R. Madhusudhan, R. Mittal, Dynamic id-based remote user password authentication schemes using smart cards: A review, Journal of Network and Computer Applications 35 (4) (2012) 1235–1248.

[25] D. Wang, Q. Gu, H. Cheng, P. Wang, The request for better measurement: A comparative evaluation of two-factor authentication schemes, in: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, ACM, 2016, pp. 475–486.

[26] D. Wang, H. Cheng, D. He, P. Wang, On the challenges in designing identity-based privacy-preserving authentication schemes for mobile devices, IEEE Systems Journal.

[27] M. Karuppiah, Remote user authentication scheme using smart card: a review, International Journal of Internet Protocol Technology 9 (2-3) (2016) 107–120.

[28] F. Wu, L. Xu, S. Kumari, X. Li, A. K. Das, M. K. Khan, M. Karuppiah, R. Baliyan, A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks, Security and Communication Networks.

[29] D. Wang, P. Wang, J. Liu, Improved privacy-preserving authentication scheme for roaming service in mobile networks, in: 2014 IEEE wireless communications and networking conference (WCNC), IEEE, 2014, pp. 3136–3141.

[30] J. Xu, W.-T. Zhu, D.-G. Feng, An improved smart card based password authentication scheme with provable security, Computer Standards & Interfaces 31 (4) (2009) 723–728.

[31] P. Kocher, J. Jaffe, B. Jun, Differential power analysis, in: Annual International Cryptology Conference, Springer, 1999, pp. 388–397.

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

[33] C.-G. Ma, D. Wang, S.-D. Zhao, Security flaws in two improved remote user authentication schemes using smart cards, International Journal of Communication Systems 27 (10) (2014) 2215–2227.

[34] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE transactions on information theory 31 (4) (1985) 469–472.

[35] R. Rivest, The md5 message-digest algorithm.

[36] Pub, NIST FIPS, 180-1,", Secure Hash Standard," National Institute of Standards and Technology, US Department of Commerce.

[37] W. Diffie, M. Hellman, New directions in cryptography, IEEE transactions on Information Theory 22 (6) (1976) 644–654.

[38] R. L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21 (2) (1978) 120–126.

[39] J. Xu, W.-T. Zhu, D.-G. Feng, An improved smart card based password authentication scheme with provable security, Computer Standards & Interfaces 31 (4) (2009) 723–728.

[40] P. Kocher, J. Jaffe, B. Jun, Differential power analysis, in: Advances in cryptologyCRYPTO99, Springer, 1999, pp. 789–789.

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

[42] C.-G. Ma, D. Wang, S.-D. Zhao, Security flaws in two improved remote user authentication schemes using smart cards, International Journal of Communication Systems 27 (10) (2014) 2215–2227.

[43] D. Wang, C.-g. Ma, P. Wang, Z. Chen, Robust smart card based password authentication scheme against smart card security breach, Cryptology ePrint Archive, Report (2012)/4392012.

[44] S. K. Sood, Secure dynamic identity-based authentication scheme using smart cards, Information Security Journal: A Global Perspective 20 (2) (2011) 67–77.

[45] J. E. Tapiador, J. C. Hernandez-Castro, P. Peris-Lopez, J. A. Clark, Cryptanalysis of song's advanced smart card based password authentication protocol, arXiv preprint arXiv:1111.2744.

[46] K.-A. Shim, Security flaws in three password-based remote user authentication schemes with smart cards, Cryptologia 36 (1) (2012) 62–69.

[47] D. He, S. Wu, Security flaws in a smart card based authentication scheme for multi-server environment, Wireless Personal Communications (2013) 1–7.

[48] D. Wang, C. Ma, D.-l. Gu, Z.-s. Cui, Cryptanalysis of two dynamic id-based remote user authentication schemes for multi-server architecture., in: NSS, Springer, 2012, pp. 462–475.

[49] D. Wang, C. Ma, P. Wu, Secure password-based remote user authentication scheme with non-tamper resistant smart cards., DBSec 12 (2012) 114–121.

[50] D. Wang, P. Wang, Offline dictionary attack on password authentication schemes using smart cards, in: Information Security, Springer, 2015, pp. 221–237.

[51] M. Karuppiah, R. Saravanan, A secure remote user mutual authentication scheme using smart cards, Journal of information security and applications 19 (4) (2014) 282–294.

[52] D. V. Klein, Foiling the cracker: A survey of, and improvements to, password security, in: Proceedings of the 2nd USENIX Security Workshop,Boston,MA,USA, 1990, pp. 5–14.

[53] M. Dell'Amico, P. Michiardi, Y. Roudier, Password strength: An empirical analysis, in: INFOCOM, 2010 Proceedings IEEE, IEEE, 2010, pp. 1–9.

[54] P. Sarkar, A Simple and Generic Construction of Authenticated Encryption with Associated Data, ACM Transactions on Information and System Security 13 (4) (2010) 33.

[55] D. Hofheinz, E. Kiltz, Practical chosen ciphertext secure encryption from factoring, in: Advances in Cryptology-EUROCRYPT 2009, Springer, 2009, pp. 313–332.

[56] V. Odelu, A. K. Das, A. Goswami, An efficient ECC-based privacy-preserving client authentication protocol with key agreement using smart card, Journal of Information Security and Applications 21 (2015) 1–19.

[57] A. K. Das, A. Goswami, A Secure and Efficient Uniqueness-and-Anonymity-Preserving Remote User Authentication Scheme for Connected Health Care, Journal of Medical Systems 37 (3) (2013) 1–16.

[58] A. K. Das, A secure and effective user authentication and privacy preserving protocol with smart cards for wireless communications, Networking Science 2 (1-2) (2013) 12–27.

[59] V. Odelu, A. K. Das, A. Goswami, An Effective and Secure Key-Management Scheme for Hierarchical Access Control in E-Medicine System, Journal of Medical Systems 37 (2) (2013) 1–18.

[60] A. Das, B. Bruhadeshwar, An improved and effective secure password-based authentication and key agreement scheme using smart cards for the telecare medicine information system, Journal of Medical Systems 37 (5) (2013) 1–17.

[61] A. K. Das, N. R. Paul, L. Tripathy, Cryptanalysis and improvement of an access control in user hierarchy based on elliptic curve cryptosystem, Information Sciences 209 (2012) 80–92.

[62] D. Mishra, A. K. Das, A. Chaturvedi, S. Mukhopadhyay, A secure password-based authentication and key agreement scheme using smart cards, Journal of Information Security and Applications 23 (2015) 28 – 43.

[63] V. Odelu, A. K. Das, A. Goswami, A secure effective key management scheme for dynamic access control in a large leaf class hierarchy, Information Sciences 269 (2014) 270–285.

[64] A. Chaturvedi, D. Mishra, S. Mukhopadhyay, An enhanced dynamic id-based authentication scheme for telecare medical information systems, Journal of King Saud University-Computer and Information Sciences 29 (1) (2017) 54–62.

[65] S. Qiu, G. Xu, H. Ahmad, L. Wang, A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems, IEEE Access xx (x) (2017) 1–13.

[66] C.-T. Li, M.-S. Hwang, Y.-P. Chu, A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks, Computer Communications 31 (12) (2008) 2803–2814.

[67] A. Kargl, S. Pyka, H. Seuschek, Fast arithmetic on atmega128 for elliptic curve cryptography., IACR Cryptology ePrint Archive 2008 (2008) 442.

[68] M. Masdari, S. Ahmadzadeh, A survey and taxonomy of the authentication schemes in telecare medicine information systems, Journal of Network and Computer Applications 87 (2017) 1–19.