International Journal of Smart Home
Vol. 9, No. 5 (2015), pp. 11-22
http://dx.doi.org/10.14257/ijsh.2015.9.5.02

An Improved Smart Card based Anonymous Multi-Server Remote User Authentication Scheme

Subhasish Banerjee[1]*, Manash Pratim Dutta[2]* and C. T. Bhunia[3]*

*Department of Computer Science & Engineering, National Institute of Technology, Arunachal Pradesh, India
subhasish.cse@nitap.in[1], manash.cse@nitap.in[2], ctbhunia@vsnl.com[3]

Abstract

As computer networks become an essential part of our daily life, therefore, protecting the resources from unauthorized users come forward with more challenging and complicated task for the researchers. From the last few decades, many number of password-based authentication schemes have been adopted in multi-server environment to protect the resources from any adversary means. Recently, Li et al. has proposed a dynamic-id based remote user authentication scheme and claimed that their scheme can provide more security than existing schemes and is suitable for practical applications. But, in this paper, we have shown that their scheme is not too much secured as they have claimed and it can suffer from stolen smart card attack, user impersonate attack and lack of some important features of smart card as well. To overcome these security flaws, we have further proposed an improved anonymous authentication scheme.

Keywords*: Authentication, Smart Card, Dynamic-id, Multi-Server*

1. Introduction

With the rapid development of the computer networks, people can easily access the remote services from any place at any time. Therefore, remote user authentication has become the most essential security mechanism to secure the network communication over insecure channels, in which password based authentication scheme is the most commonly used technique. Such scheme provides an efficient and accurate way for the remote server to verify the authenticity of a remote user. In 1981, Lamport [1] and Lemon et al. [2] proposed first conventional authentication system in which the remote server maintained a password table to verify legitimacy of users. However, these schemes suffer not only from hacking or modifying password table but also increase the system overhead of maintaining or protecting such tables. To overcome such kind of risks and due to their low cost, cryptographic capacity and portability, smart cards have been widely adopted in remote user authentication schemes [4-13, 23-25]. However, most of them are still insecure against some set of attacks and later some improved schemes [4-5, 11] have also been introduced. In addition, since the number of service provider server for users is usually more than one, remote user authentication schemes used for multi-server architecture rather than single server circumstance is considered. With a single registration, many number of authentication schemes have been designed [13-14] in multi-server environment. But, most of the proposed schemes have a common feature that is, the user's identity is kept static during entire communication over the insecure channels which may cause the leakage of some information about the user and can create the risk of ID-theft during the message transmission. To overcome such risks and make the identity dynamic in nature, many researchers have proposed various remote user authentication schemes based on dynamic-ID [15-20, 23-25]. However, most of them are still insecure against stolen verifier attack, denial of service attack, password guessing attack, insider attack and also lack of some important security requirements such as,

ISSN: 1975-4094 IJSH

session key agreement, forward secrecy etc [22]. Recently, Lee et al. [21] has proposed a remote user authentication scheme based on dynamic-ID and claimed that, with preserving user anonymity can resist various kinds of attacks as well. Unfortunately, Li et al. [23] has showed that their scheme can't achieve the proper authentication and can suffer from various well known attacks and has further proposed an improved dynamic ID based remote user authentication scheme in multi server architecture and has defined that their scheme can resist against all well known attacks and provides the proper authentication, forward secrecy and known key secrecy. But, during our research, we have found that the proposed scheme is not as much secured as they have claimed. That is, if the attacker extracts the secret information from the stolen smart card by any means, then adversary can easily guess the correct password PW and real identity ID by eavesdropping any previous login request message, without knowing the master secret key x, that is stolen smart card attack and also fails to resist user impersonates attack. Moreover, they have overlooked one of the important features of the smart card that is, in the case of lost or stolen smart card there must be some provisions by which user can invalidate the stolen one and issue a new smart card i.e. smart card revocation mechanism. To overcome such weaknesses and missing features, we have proposed a secure and improved anonymous remote user authentication scheme for multi server environments which can solve not only all the identified security weaknesses but also satisfies more functionality features. The rest of this paper is organized as follows. Section 2 and 3 contain the review of Li et al.'s scheme and their flaws respectively. Our improved scheme is presented in section 4. In section 5, we have analyzed the security mechanism of our proposed scheme and compared the functionality features of our scheme with related schemes in section 6. Lastly, we have completed our paper with conclusion and future work in section 7.

2. Overview of Li *et al.'s* Scheme

We have used most of the notations of Li *et al*.'s scheme throughout this paper, which are summarized in Table-1. Here, we will review Li *et al*.'s remote user authentication scheme under multi-server environments. Their scheme has four phases, namely, registration, login, verification and password change phase. We explain the registration, login and verification phases only as we will use them to carry out cryptanalysis in section 3. In their scheme, the trusted registration center RC uses to choose the master secret key x and a secret number y to compute two secret information $h(x||y)$ and $h(SID_j||h(y))$, and then passes them to S_j through a secure channel. The complete steps are defined as follows:

2.1 User Registration Phase

Before accessing the remote server S_j, the remote users U_i must register themselves to registration center RC. The details of this phase are defined below:

i). U_i uses to choose his/her identity ID_i, the password PW_i, and computes $A_i = h(b \oplus PW_i)$, where b is a random number generated by U_i. Then U_i sends the message $\{ID_i, A_i\}$ to the RC through a secure channel for further operation and to generate the user's smart card.

ii). Registration center computes $B_i = h(ID_i||x)$, $C_i = h(ID_i||h(y)||A_i)$, $D_i = h(B_i||h(x||y))$ and $E_i = B_i \oplus h(x||y)$, then stores the values of C_i, D_i, E_i, h(.) and h(y) in the smart card and forwards this through a secure channel and finally U_i safely stores b into it.

Table 1. Notations and Definition used in this Paper

Notation	Definitions
U_i	i^{th} user
S_j	j^{th} server
RC	Trusted Registration Center
ID_i	Unique identification of U_i
PW_i	Password of U_i
SID_j	Unique identification of S_j
CID_i	Dynamic ID generated by U_i to preserve user anonymity
h(.)	A one-way collision resistant hash function
x, y	The master secret key and the secret number respectively of RC
$\oplus$	The bitwise XOR operation
$\|\|$	The concatenation operation

2.2 User Login and Authentication phase

In this phase, the user U_i inserts his/her smart card and enters the identification and password ID_i and PW_i respectively to initiate the login phase. The steps which are involved to verify the authenticity of the user and remote server and to make agreement for a common session key for further communication are given as follows:

i). After providing ID_i and PW_i, smart card computes $A_i = h(b \oplus PW_i)$, $C_i^* = h(ID_i||h(y)||A_i)$, and checks whether the computed C_i^* is equal to stored C_i or not. If they are, U_i proceeds to the next steps for further computation to generate the login request message. Otherwise, the smart card aborts the session.

ii). Smartcard computes $P_{ij} = E_i \oplus h(h(SID_j||h(y))||N_i)$, $CID_i = A_i \oplus h(D_i||SID_j||N_i)$, $M_1 = h(P_{ij}||CID_i||D_i||N_i)$ and $M_2 = h(SID_j||h(y)) \oplus N_i$, where N_i is the nonce generated by the smart card and sends the login request message $\{P_{ij}, CID_i, M_1, M_2\}$ to S_j.

iii). After receiving the message, S_j computes $N_i = h(SID_j||h(y)) \oplus M_2$, $E_i = P_{ij} \oplus h(h(SID_j||h(y))||N_i)$, $B_i = E_i \oplus h(x||y)$, $D_i = h(B_i||h(x||y))$ and $A_i = CID_i \oplus h(D_i||SID_j||N_i)$ using pre-shared secret information $h(SID_j||h(y))$ and $h(x||y)$ from RC.

iv). S_j further computes $h(P_{ij}||CID_i||D_i||N_i)$ and verifies whether it is matched with M_1 or not. If they are not matched, S_j rejects the login request and terminates this session. Otherwise, S_j accepts the login request message and computes $M_3 = h(D_i||A_i||N_j||SID_j)$, $M_4 = A_i \oplus N_i \oplus N_j$, where nonce N_j is generated by S_j. Finally, S_j sends the message $\{M_3, M_4\}$ to U_i as a reply message.

v). Once the message has been received, U_i computes $N_j = A_i \oplus N_i \oplus M_4$, and verifies whether $h(D_i||A_i||N_j||SID_j)$ is matched with M_3 or not. If it is matched, U_i will authenticate the server S_j as a valid server and computes the mutual authentication message $M_5 = h(D_i||A_i||N_i||SID_j)$ and sends the same to the server S_j for mutual authentication.

vi). After receiving the message from U_i, S_j computes $h(D_i||A_i||N_i||SID_j)$ and verifies with the received message $\{M_5\}$. If they are equal, S_j successfully authenticates U_i and the mutual authentication is completed. After the mutual authentication phase, the user U_i and the server S_j compute $Sk = h(D_i||A_i||N_i||N_j||SID_j)$, which is considered as their session key for future secure communication.

3. Flaws of Li *et al.*'s Scheme

Although Li *et al*. [23] have claimed that their scheme is much secured and resists various kinds of well known attacks but, we have proved that their scheme is not that much secured as they have claimed and suffers from stolen smart card attack and user impersonate attack, also does not support the revocation of stolen or lost smart card. The details of our analysis are given below:

3.1 Stolen Smart Card Attack

In security analysis section, they have claimed that even if the attacker extracts the secret information $\{C_i, D_i, E_i, b, h(.), h(y)\}$ from the lost or stolen smart card of user U_i by some means, then also the attacker cannot guess the correct values of identity ID_i and password PW_i in real polynomial time without the knowledge of master secret key x, as they are protected by one way hash function. However, in this section, we have showed that if the attacker succeeds to extract the secret data from the lost or stolen smart card, then the attacker can guess the same successfully by intercepting any previous U_i's login request from any given session, without the knowledge of master secret key x. Cryptanalysis steps are defined as follows:

i). The attacker Z obtains the secret values $\{C_i, b, D_i, h(y)\}$ from the lost smart card and eavesdrop any previous login message $\{CID_i, P_{ij}, M_1, M_2\}$ during the transmission at any given session.

ii). Z computes the nonce $N_i = M_2 \oplus h(SID_j \,||\, h(y))$, $E_i = P_{ij} \oplus h(h(SID_j||h(y))||N_i) = B_i \oplus h(x||y)$ and $A_i = CID_i \oplus h(D_i||SID_j||N_i) = h(b \oplus PW_i)$, where SID_j is a known parameter.

iii). Z guesses a password PW_z of victim party U_i and computes $h(b \oplus PW_z)$, and compares with calculated value of A_i. If it holds, it indicates that $PW_z = PW_i$. Z can exhaustively examine all possible passwords PW_z of U_i, until he finds the correct one.

iv). After successful guessing of a password, Z can also predict the original identity ID_z of victim party U_i and computes $h(ID_z||h(y)||A_i)$, and compares with obtained secret value C_i from the lost smart card. If it holds, it indicates that $ID_z = ID_i$. Z can exhaustively examine all possible identity ID_z of U_i, until he finds the intended one.

From the above analysis, we can observe how successfully the adversary can guess the real identity and password without any knowledge about the master secret key x, but extracting only the secret information from the lost or stolen smart card and intercepting any previous login request. As the speed of computational process is not being limited any more; difficulty of exhaustive searching for such secret parameters may not survive. Hence, their scheme cannot resist stolen smart card attack.

3.2 User Impersonates Attack

Assume that adversary Z extracts the secret parameters $\{C_i, D_i, E_i, b, h(.), h(y)\}$ from the smart card and eavesdrop any previous login request message $\{CID_i , P_{ij} , M_1, M_2\}$ during the communication between U_i and server S_j, then adversary can impersonate himself as a valid user by easily creating a forge login message to fool a server S_x without knowing PW_i. Here, S_x is any service providers sever and can be server S_j too. To apply such attack, the attacker Z can perform the following steps:

i). Z calculates random nonce which is generated by U_i that is, $N_i = M_2 \oplus h(SID_j \,||h(y))$ and secret values $E_i = P_{ij} \oplus h(h(SID_j||h(y))||N_i)$ and $A_i = CID_i \oplus h(D_i||SID_i||N_i)$, where SID_j is a known parameter.

ii). To create forge login request message, the attacker Z can compute $P'_{ix} = E_i \oplus h(h(SID_x||h(y))||N_z)$, $CID'_i = A_i \oplus h(D_i||SID_x||N_z)$, $M'_1 = h(P'_{ix}||CID'_i||D_i||N_z)$, $M'_2 =$

$h(SID_x||h(y))\oplus N_z$, and sends $\{P'_{ix}, CID'_i, M'_1, M'_2\}$ a forge login request to the server S_x.

iii). Once the message has been received, the server S_x computes $N_z = M'_2 \oplus h(SID_x||h(y))$, $E'_i = P'_{ix} \oplus h(h(SID_x||h(y))||N_z)$, $B'_i = E'_i \oplus h(x||y)$, $D'_i = h(B'_i||h(x||y))$ and $A'_i = CID'_i \oplus h(D'_i||SID_x||N_z)$, then checks whether $h(P'_{ix}||CID'_i||D'_i||N_z)$ is matched with M'_1 or not. As the attacker does not replace any values except SID_x and N_z, it will be verified successfully and S_x generates random nonce N_x and computes $M'_3=h(D'_i||A'_i||N_x||SID_x)$, $M'_4 = A'_i \oplus N_z \oplus N_x$ and forwards the message $\{M'_3, M'_4\}$ to Z.

iv). After receiving $\{M'_3, M'_4\}$, Z computes $N_x = M'_4 \oplus A_i \oplus N_z$, and $M'_5=h(D_i||A_i||N_x||SID_x)$, and submits $\{M'_5\}$ to S_x for mutual authentication.

v). Upon receiving the message M'_5, S_x computes $h(D'_i||A'_i||N_z||N_x)$. It is obvious that $h(D'_i||A'_i||N_x||SID_x) = h(D_i||A_i||N_x||SID_x) = M'_5$, so S_x will successfully authenticate Z as a legal user U_i and at the end, the attacker Z and S_x share a common session key $Sk= h(D_i||A_i||N_z||N_x) = h(D'_i||A'_i||N_z||N_x)$.

From the above analysis, we can see that if the adversary gets the secret information from the user's smart card by some ways and eavesdrop any previous login request then adversary Z can easily impersonate as a legal user U_i and shares a session key Sk with the server S_x. So, Li *et al.*'s scheme is unsuccessful to resist against user impersonates attack.

3.3 Revocation of User's Lost or Stolen Smart Card

It should be one of the important features of the smart card based authentication scheme [22] that in case if the smart card is lost or stolen; there should have a provision of invalidating the lost or stolen smart card and generates a new one, otherwise an adversary can impersonate as valid registered user, as we have seen from the above mentioned attacks. So, if we succeed to keep the record of valid card identifier of each registered user anyhow, then it can be distinguished very easily from valid card to invalid one. Unfortunately, Li *et al.*'s scheme has overlooked this feature and there is no prerequisite to revoke the lost smart card. Thus, their scheme has major flaws to provide the important feature of smart card based authentication for revoking the lost smart card without changing the user identities.

4. Proposed Scheme

Here, we have proposed an improved anonymous authentication scheme using smart card to eliminate the weaknesses and flaws of Li *et al.*'s scheme. The proposed scheme uses the same notations as mentioned in Table-1. The improved scheme has an extra phase as compared to Li *et al.*'s scheme which is smart card revocation phase. The proposed scheme also has the three participants - the user U_i, registration center RC and authentication server S_j. After choosing the master secret key x and secret number y, the registration center RC computes h(x||y) and h(y), and shares these with the server S_j through a secure channel. The detailed descriptions of these phases are defined as:

4.1 Registration Phase

This phase is invoked, when a new user U_i wants to access the service from remote servers or reregister for revocation of stolen smart card. The new user U_i and registration center RC need to perform the following steps:

i). A user U_i chooses his ID_i, the password PW_i, and computes password digest $RPW_i = h(b\oplus PW_i)$, where b is a random number generated by U_i. Then U_i sends ID_i and RPW_i to the RC for registration through a secure channel.

ii). After receiving the registration request message, RC verifies whether the chosen ID_i already exists in the registration record database or not. If so, RC initiates U_i to choose another ID_i. In addition, RC checks the registration record of U_i and if U_i is a new user then RC sets the value of N=0. Otherwise, if U_i is reregistering then RC increments the value of N by one and stores the values of ID_i and N in the database. Then RC computes the following steps and is also depicted in Fig. 1.

$A_i = h(x||IDU)$, where $IDU= (ID_i||N)$
$B_i = h(ID_i||h(y)||RPW_i) \oplus A_i$
$V_i = h(A_i||h(y)||RPW_i)$
$D_i = h(A_i \oplus h(x||y))$
$E_i = A_i \oplus h(x||y)$

iii). Lastly, RC stores $\{B_i, V_i, D_i, E_i, h(y), h(.)\}$ to the memory of U_i's smart card and sends to the user through a secure channel.
iv). Upon receiving the smart card, U_i securely stores b and it finally contains $\{B_i, V_i, D_i, E_i, h(y), h(.), b\}$.

These above steps complete the registration process of the remote user.

4.2 User Login Phase

This is the phase when the remote user U_i interacts with the system and wants to access from the remote server S_j. U_i inserts his smart card into the card reader and inputs his identity and password ID_i and PW_i respectively and then the smart card performs the following steps to generate the login request message:

i). Smart card computes $RPW_i = h(b \oplus PW_i)$, $A_i = B_i \oplus h(ID_i||h(y)||RPW_i)$ and $V_i^* = h(A_i||h(y)||RPW_i)$, where random number b and h(y) are securely pre-stored in the smart card, and checks whether the computed V_i^* is matched with V_i or not. If verification succeeds then proceeds to next step, otherwise smart card rejects the login request.
ii). After the confirmation of authenticity about the smart card with user U_i, smart card further computes:

$P_{ij} = E_i \oplus h(SID_j||h(y)||N_i)$
$CID_i = RPW_i \oplus h(D_i||SID_j||N_i)$
$C_1 = h(A_i||D_i||CID_i||N_i)$
$C_2 = h(SID_j||h(y)) \oplus N_i$

where nonce N_i is generated by the smart card and at the end of login phase, U_i sends the login request message $\{CID_i, P_{ij}, C_1, C_2\}$ to S_j for authentication.

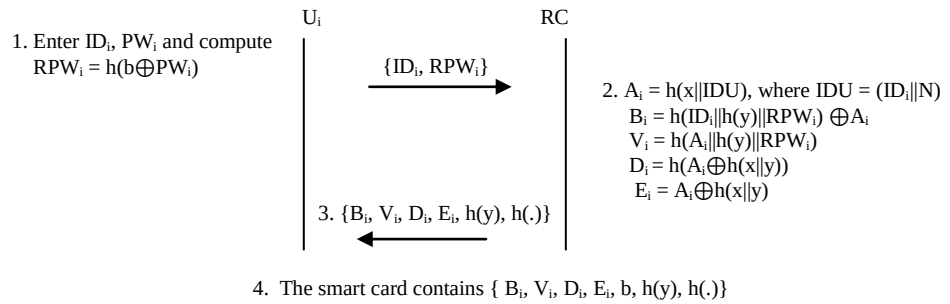

Figure 1. The Registration Phase of our Scheme

4.3 Authentication Phase

Once the message has been received, the server S_j verifies the authenticity about the received message by the following steps:

i). Authentication server S_j computes $N_i = C_2 \oplus h(SID_j||h(y))$, $E_i = P_{ij} \oplus h(SID_j||h(y)||N_i)$, $A_i = E_i \oplus h(x||y)$, $D_i = h(A_i||h(x||y))$ and $RPW_i = CID_i \oplus h(D_i||SID_j||N_i)$ by using $\{CID_i, P_{ij}, C_1, C_2\}$, and shared secret values h(y) and h(x||y).
ii). S_j further computes $h(A_i||D_i||CID_i||N_i)$ and compares with received C_1. If it does not match, S_j simply rejects the login request and terminates this session. Otherwise, S_j generates a random nonce N_j and computes $C_3 = h(SID_i||D_i||RPW_i||N_j)$, $C_4 = RPW_i \oplus N_i \oplus N_j$ and sends the message $\{C_3, C_4\}$ to U_i.
iii). After receiving the message $\{C_3, C_4\}$ from S_j, U_i computes $N_j = C_4 \oplus RPW_i \oplus N_i$ and compares $h(SID_j||D_i||RPW_i||N_j)$ with received C_3. If it does not hold, U_i rejects these messages and terminates this session. Otherwise, U_i authenticates the remote server S_j and computes the mutual authentication message $C_5 = h(SID_j||N_i||RPW_i||D_i)$. Finally, U_i sends the message $\{C_5\}$ to S_j for mutual authentication.
iv). Upon receiving the message $\{C_5\}$, S_j computes $h(SID_j||N_i||RPW_i||D_i)$ and compares with received C_5. If they are equal, S_j authenticates the user U_i successfully and accepts the login request.

At the end of this phase, the remote user U_i and the server S_j make an agreement on session key $Sk = h(RPW_i||D_i||SID_j||N_i||N_j)$ for making any further communication during that session. The login and authentication mechanisms have also been shown in Fig. 2.

4.4 Password Updating Phase

In this phase, whenever the U_i feels to update his/her old password PW_i with the new one PW_i^{new}, then he/she must follow the following steps to fulfill the requirement:

i). After inserting the smart card into the smart card reader, the user enters ID_i and PW_i, and requests to change the password.
ii). U_i's smart card computes $RPW_i = h(b \oplus PW_i)$, $A_i = B_i \oplus h(ID_i||h(y)||RPW_i)$ and $V_i^* = h(A_i||h(y)||RPW_i)$.
iii). U_i's smart card verifies whether V_i^* is matched with stored parameter V_i or not.
iv). If it succeeds, then U_i selects the new password PW_i^{new} and proceeds to the next step, otherwise the smart card simply rejects the request.
v). U_i's smart card computes $RPW_i^{new} = h(b \oplus PW_i^{new})$, $B_i^{new} = h(ID_i||h(y)||RPW_i^{new}) \oplus A_i$ and $V_i^{new} = h(A_i||h(y)||RPW_i^{new})$, and then replaces B_i and V_i with B_i^{new} and V_i^{new} respectively. At the end of this step, the password will be successfully updated.

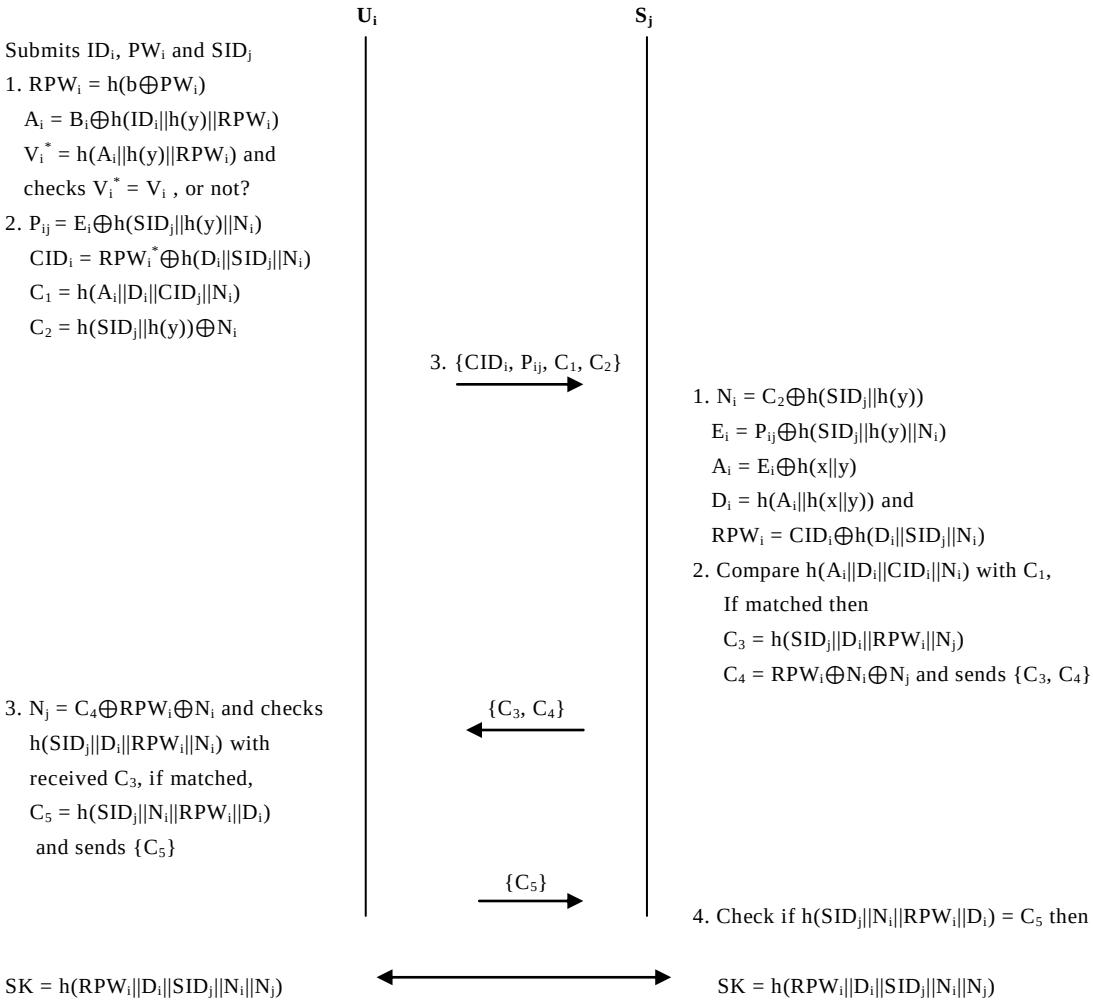

Figure 2. Login, Authentication and Session Key Agreement of Proposed Scheme

4.5 Revocation of User's Lost or Stolen Smart Card

During our registration phase, the RC stores secret credentials N against each user ID in their database. Whenever the user U_i sends the request to invalidate the older smart card and generates a new one, by proving his/her authenticity about the smart card (for example, by providing his/her first school name, date of birth etc.), RC updates the stored credentials by incrementing the value of N by 1 and follows the same procedure as defined in registration phase to issue a new smart card. So, at the end of this phase, user U_i will have a new smart card with the updated secret information. Hence, it is impossible to make any hamper by the adversary with the lost or stolen old smart card as all the parameters of the smart cards have already been changed with the new value of N.

5. Security Analysis

S1. Protection Against Stolen Smart Card Attack

In our scheme, even if the attacker somehow extracts the secret information $\{B_i, V_i, D_i, E_i, h(y), b, h\}$ from the lost or stolen smart card and eavesdrop any previous login request $\{CID_i, P_{ij}, C_1, C_2\}$ then also it will be infeasible to compute any forge login request that can pass the authentication phase successfully without knowing ID_i and RPW_i. However,

to change the user password or login to the system, adversary can compute $N_i = C_2 \oplus h(SID_j||h(y))$, $E_i = h(SID_j||h(y)||N_i) \oplus P_{ij} = A_i \oplus h(x||y)$ and $RPW_i = CID_i \oplus h(D_i||SID_j||N_i)$ and may guess the correct password PW_i from RPW_i, by exhaustively examining all possible password combinations PW_z of U_i. Even after guessing the password successfully, attacker cannot guess the correct ID_i without knowing A_i, where A_i is hidden in E_i. So, it is impossible to compute the correct value of A_i without knowing master secret key h(x||y). Hence, no one can either create the fake login request or can guess the correct ID_i and PW_i in the same polynomial time. Therefore, the proposed scheme is secured against stolen smart card attack.

S2. Protection Against Replay Attack

The adversary may replay any previous intercepted login request message from the valid user and response message from the server to cheat user U_i or server S_j. In the proposed scheme, two random numbers N_i and N_j are used to make the communication message dynamic in nature and will remain valid for a session only. Suppose, the attacker Z, after intercepting any previous login request $\{CID_i, P_{ij}, C_1, C_2\}$ from the user U_i, may replay this message to S_j to access the services. Z will receive the acknowledge message $\{C_3, C_4\}$ from the server S_j. However, Z cannot compute mutual message $\{C_5\}$ to respond to the server S_j without knowing A_i, B_i and N_i. Even if Z responds to the server S_j, by replaying the intercepted previous mutual message $\{C_5\}$, S_j computes $h(SID_j||N_i||RPW_i||D_i)$ and will compare it with the received message $\{C_5\}$. As Z replays intercepted login request message and mutual message $\{C_5\}$ of the same session, so computed value will be matched with C_5. But Z, cannot establish the session key agreement with the server S_j without knowing RPW_i, D_i, N_i and N_j.

Similarly, if the attacker tries to cheat the user U_i by sending intercepted message $\{C_3, C_4\}$ from the server S_j, in this session, then computed value of $h(SID_j||D_i||RPW_i||N_j)$ will not be equal to C_3 because the two random numbers N_i of these two different sessions will not be equal. Thus, the computed N_j will not be matched with random number N_j in this session which was earlier generated by S_j. Hence, the proposed scheme is secured against replay attack.

S3. Protection Against User Impersonates Attack

After modifying the intercepted message, an attacker can try to prove himself as legal user to access the services from remote server S_j. To do so, the attacker must be able to create a valid forge login request $\{CID_i, P_{ij}, C_1, C_2\}$ to fool S_j. However, it is infeasible to compute such login request without knowing the secret information A_i, RPW_i, D_i, E_i, h(y) and N_i.

On the other hand, if an adversary is a registered but malicious user then also he cannot prove himself as another legal user. Even though if he will try with any intercepted previous login message and his smart card, then also it will be impossible to compute D_i and RPW_i without knowing h(x||y), b and PW_i.

Similarly, if anyhow the attacker gets the victim's smart card and retrieves the secret information $\{B_i, V_i, D_i, E_i, h(y), b, h\}$ still the attacker cannot create any forge login request to fool S_j with any previous login request message $\{CID_i, P_{ij}, C_1, C_2\}$. Since, he cannot use these parameters to get the correct value of A_i from the extracted value E_i without knowing h(x||y) therefore, it is impossible to create any forge message C_1, which can pass the verification successfully at the authentication phase. Hence, our proposed scheme can successfully protect against user impersonates attack.

S4. Protection against Insider Attack

In this attack, a privileged insider of the RC can access other server by stealing the identity and password verifier from the RC's verification table. However, in the proposed

scheme, U_i registers himself to RC by presenting $RPW_i = h(b \oplus PW_i)$ instead of PW_i and $h(PW_i)$. During registration, the value of b is not disclosed to RC, so the insider of RC cannot get PW_i by performing any kind of guessing attack on RPW_i. However, the proposed scheme does not maintain any verification table except the registration record table. Therefore, the proposed scheme can successfully withstand in insider attack.

S5. Revocation of User's Lost or Stolen Smart Card

The proposed scheme has an additional feature as compared to Li *et al.*'s [23] scheme. In our scheme, the registered user U_i can invalidate the lost or stolen smart card and issues a new smart card with the new set of information. Whenever the user U_i sends the request to RC for revocation of lost or stolen smart card by proving his/her authenticity, the RC increments the value of N by one in its registered record database and computes new value of A_i, B_i, V_i, D_i, and E_i, and issues a new smart card to U_i. So, if an adversary tries to hamper the user U_i using the lost or stolen smart card to login into the system, then cannot prove himself as a valid user due to the changes in registered record database of N. So, lost or stolen smart card will become useless to be used further.

S6. Perfect Forward Secrecy

In this scheme, if the secret information h(x||y) and h(y) have been compromised by any means, then also it is impossible to compute a valid forge login request message $\{CID_i, P_{ij}, C_1, C_2\}$ by an adversary without knowing user's RPW_i and A_i. So, our proposed scheme can provide the perfect forward secrecy.

5. Performance and Security Comparison

In this section, we have discussed the security features and performance issues of our scheme with other related existing schemes, which are summarized in Table-2 and Table-3 respectively. From Table-2, we can analyze that our scheme provides more security and higher functionality features as compared to other schemes. Because of very less computational cost incurred by bitwise XOR and concatenation, we have not added these two operations in our account for comparison purpose. We can see from Table-3 that, our scheme has been designed by adding one extra hash function as compared to Li *et al.*'s scheme and but as same as Lee *et al.*'s. Besides, our scheme can provide better security and strongly resists against stolen smart card attack and user impersonates attack and also has additional features of smart card revocation too. Hence, our scheme is more secured and robust than compared schemes.

Table 2. Security Features Comparison

Security characteristics	S1	S2	S3	S4	S5	S6
X. Li *et al.*'s[23]	No	Yes	No	Yes	No	Yes
Lee *et al.*'s [21]	Yes	Yes	No	Yes	No	Yes
Our Proposed scheme	Yes	Yes	Yes	Yes	Yes	Yes

Table 3. Performance Comparison with Other Related Schemes

Phases	X. Li *et al.*'s [23]	Lee *et al.*'s [21]	Proposed Scheme
Registration Phase	$6T_H + 2T_X$	$6T_H + 2T_X$	$7T_H + 2T_X$
Login Phase	$7T_H + T_X + T_C$	$7T_H + T_X + T_C$	$7T_H + T_X + T_C$
Authentication Phase	$10T_H + 2T_X + 3T_C$	$11T_H + 2T_X + 3T_C$	$10T_H + 2T_X + 3T_C$
Total	$23T_H + 5T_X + 4T_C$	$24T_H + 5T_X + 4T_C$	$24T_H + 5T_X + 4T_C$

Where T_H: Time required for hash operation, T_C: Time required for comparison and T_X: Communication cost for login.

7. Conclusion

As the remote user authentication scheme becomes a great research challenge over the insecure communication channel, many schemes have been proposed to provide the higher level of security and with many numbers of features. Li. et al. proposed a scheme where the remote user can be authenticated very easily and securely by preserving the user anonymity under multi-server environments. In this paper, we have reviewed and proved that their scheme has some major security weaknesses and cannot withstand against some well known attacks. In order to remove such weaknesses and to enhance the security in large scale, an improved scheme has also been introduced. This scheme consists of some more additional features and provides the perfect security against the well known attacks. Therefore, the proposed scheme is well suited for practical applications.

References

[1] L. Lamport, "Password authentication with insecure communication", Communications of the ACM, vol. 24, no. 11, **(1981)**, pp. 770-772.
[2] R. E. Lemon, S. M. Matyas and C. H. Meyar, "Cryptographic authentication of time-invariant quantities", IEEE Trans. Communication, vol. 29, **(1981)**, pp. 773-777.
[3] M. S. Hwang, L. H. Li, "A new remote user authentication scheme using smart cards", IEEE Transaction on Consumer Electronics, vol. 46, no. 1, **(2000)**, pp. 28-30.
[4] E. J. Yoon, E. K. Ryu and K. Y. Yoo, "Further improvement of an efficient password based remote user authentication scheme using smart cards", IEEE Transaction on Consumer Electronics, vol. 50, no. 2, **(2004)**, pp. 612-614.
[5] M. L. Das, A. Saxena and V. P. Gulati, "A dynamic ID-based remote user authentication scheme", IEEE Transaction on Consumer Electronics, vol. 50, no. 2, **(2004)**, pp. 629-631.
[6] C. W. Lin, C. S. Tsai and M. S. Hwang, "A new strong password authentication scheme using one-way Hash functions", Journal of Computer and Systems Sciences International, vol. 45, no. 4, **(2006)**, pp. 623-626.
[7] C. S. Bindu, P. Reddy and B. Satyanarayana, "Improved remote user authentication scheme preserving user anonymity", International Journal of Computer Science and Network Security, vol. 83, **(2008)**, pp. 62-66.
[8] L. Fan, J. H. Li and H. W. Zhu, "An enhancement of timestamp-based password authentication scheme", Computer Security, vol. 21, no. 7, **(2002)**, pp. 665-667.
[9] J. J. Shen, C. W. Lin and M. S. Hwang, "Security enhancement for the timestamp-based password authentication using smart cards", Computer Security, vol. 22, no. 7, **(2003)**, pp. 591-595.
[10] C. T. Li and M. S. Hwang, "An efficient biometric based remote user authentication scheme using smart cards", Journal on Networking and Computer Applications, vol. 33, **(2010)**, pp. 1-5.
[11] A. K. Das, "Analysis and improvement on an efficient biometric based remote user authentication scheme using smart cards", IET Information Security, vol. 5, no. 3, **(2011)**, pp. 541-552.
[12] C. H. Lin and Y. Y. Lai, "A flexible biometric remote user authentication scheme", Computer Standards and Interfaces, vol. 27, no. 1, **(2004)**, pp.19-23.
[13] L. H. Li, L. C. Lin and M. S. Hwang, "A remote password authentication scheme for multi-server architecture using neural networks", IEEE Transaction on Neural Networks, vol. 12, **(2001)**, pp. 1498-1504.
[14] W. S. Jung, "Efficient multi server-password authentication key agreement using smart cards", IEEE Transactions on Consumer Electronics, vol. 50, **(2004)**, pp. 251-255.
[15] M. L. Das, A. Saxena and V. P. Gulati, "A dynamic ID-based remote user authentication scheme", IEEE Transactions on Consumer Electronics, vol. 50, no. 2, **(2004)**, pp. 629-631.
[16] I. Liao, C.C. Lee and M. S. Hwang, "Security enhancement for a dynamic ID-based remote user authentication scheme", Proceeding of the international conference on next generation web services practices, NWeSP, **(2005)**; Seoul, Korea.
[17] Y. P. Liou, J. Lin and S. S. Wang, "New dynamic ID-based remote user authentication scheme using smart cards", Proceedings of 16th information security conference, **(2006)**; Taiwan.
[18] E. J. Yoon and K. Y. Yoo, "Improving the dynamic ID-based remote mutual authentication scheme", Proc. OTM Workshops, LNCS 4277, Springer, **(2006)**.
[19] Y. Y. Wang, J. Y. Kiu, F. X. Xiao and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme", Computer Communications, vol. 32, no. 4, **(2009)**, pp. 583-585.
[20] M. K. Khan, S. K. Kim and K. Alghathbar, "Crypyanalysis and security enhancement of a more efficient and secure dynamic ID-based remote user authentication scheme", Computer Communication, vol. 34, **(2011)**, pp. 305-309.

[21] C. C. Lee, T. H. Lin and R. X. Chang, "A secure dynamic ID based remote user authentication scheme for multi-server environments using smart card", Expert system with applications, vol. 38, no. 11, **(2011)**, pp. 13863-13870.
[22] R. Madhusudhan and R. C. Mittal, "Dynamic Id-based remote user password authentication schemes using smart cards: A review", Journal of Network and Computer Application, vol. 35, no. 4, **(2012)**, pp. 1235-1248.
[23] X. Li, J. Ma, W. Wang, Y. Xiong and J. Zhang, "A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments", Mathematical and computer Modeling, vol. 58, no. 1-2, **(2013)**, pp. 85-95.
[24] K. Ch. Baruah, S. Banerjee, M. P. Dutta and C. T. Bhunia, "An Improved Biometric-based Multi server Authentication Scheme using Smart Card", International Journal of Security and Its Application, vol. 9, no. 1, **(2015)**, pp. 397-408.
[25] S. Banerjee, M. P. Dutta and C. T. Bhunia, "Cryptanalysis and Security Enhancement of an Efficient and Secure Dynamic ID Based Remote User Authentication Scheme for Multi-Server Environments", Proceedings of the International Conference on Advanced Research in Computer Science Engineering & Technology (ICARCSET), **(2015)**; Eluru, India.

Authors

Subhasish Banerjee, he received his M.Tech degree in Computer Application from Indian School of Mines, Dhanbad, India in 2012. Currently he is persuing his Ph.D and also working as Assistent Professor in the Department of Computer Science and Engineering in National Institute of Technology, Arunachal Pradesh. His research activities are mainly focused on crytography and infornation secutity.

Manash Pratim Dutta, he received his M.Tech degree in Information Technology from Sikkim Manipal University, Sikkim, India in 2012. Currently, he is working as Assistent Professor and persuing his Ph.D in the Department of Computer Science and Engineering in National Institute of Technology, Arunachal Pradesh. His research activities are mainly focused on crytography and infornation secutity.

Chandan Tilak Bhunia, he did his B. Tech. in Radiophysics and Electronics in 1983 from Calcutta University. He received his M. Tech. in Radiophysics and Electronics in 1985 and then joined North Bengal University as a lecturer of Computer Science & Applications in 1988. He became Assistant Professor of ECE at NERIST, Govt. of India in 1990. He got P. hd. in Computer Science & Engineering from Jadavpur University. He became a full Professor in 1997 at NERIST. Currently, he is working as a Director of National Institute of Technology, Arunachal Pradesh. He has published around 150 research papers in various national and internatiol journals of repute. Under his supervision, five P. hd. scholars got awarded and nine scholars are currently working in various fields.

