International Journal of Information & Network Security (IJINS)
Vol.3, No.6, December 2014, pp. 343~352
ISSN: 2089-3299 ❒ 343

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

Subhasish Banerjee*, Manash Pratim Dutta*, C. T. Bhunia*
* Departement of Computer Science & Engineering, National Institute of Technology

Article Info

Article history:

Received Jun 12th, 2014
Revised Aug 20th, 2014
Accepted Aug 26th, 2014

Keyword:

authentication
smart card
dynamic-id
multi-server

ABSTRACT

As computer networks becomes an essential part of our daily life, protecting the resources from unauthorized users come forward with more challenging and complicated task for researchers. From the last few decades, many numbers of password-based authentication schemes have been adopted in multi-server environment to protect the resources from any adversary means. Recently, X. Li et al. proposed a dynamic-id based remote user authentication scheme and claimed that their scheme can provides more security than existing schemes and suitable for practical application. But, in this paper we have shown that, their scheme is not too much secure as they claimed and it can suffer from stolen smart card attack, user impersonate attack and lacking of some important features of smart card as well. To overcome these security flaws, we propose an improved anonymous authentication scheme, which can remove not only all the identified security weakness but also satisfies more functionality features.

Corresponding Author:

Subhasish Banerjee,
Departement of Computer Science & Engineering,
National Institute of Technology
Arunachal Pradesh, Yupia-791110, India.
Email: subhasishism@gmail.com

1. INTRODUCTION

With the rapid development of the computer networks, people can access the services from any place and at any time. Therefore, remote user authentication has become most essential security mechanism to secure network communication over an insecure channel, in which password based authentication scheme is the most commonly used technique. Password based authentication scheme provides an efficient and accurate way for the remote server to verify the authenticity of a user. In 1981, Lamport [1] and Lemon et al. [2] proposed first conventional authentication system in which the remote server maintains a password table to verify legitimacy of users. However, these schemes suffer not only from the hacking and modifying password table but also suffer from 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]. However, most of them are still vulnerable to some set of attacks and further some improved schemes [4-5, 11] have also been proposed. In addition, since number of servers providing the facilities for users is usually more than one, remote user authentication schemes used for multi-server architectures rather than single server circumstance is considered. With only 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, in all the communication over insecure channels user's identity is static, which may cause the leakage of some information about the user and can create risk of ID-theft during the message transmission. To remove such a risk and make the identity in dynamic in nature many researchers have proposed remote user authentication schemes based on dynamic-ID [15-20, 23]. However, most of them are still insecure against stolen verifier attack, denial of service attack, password guessing attack, insider attack and also has some missing important security requirements such as, session key agreement, forward secrecy etc [22]. Recently, C.C. Lee et al. [21] proposed a remote user authentication scheme based on dynamic-ID and claimed that, with preserving user anonymity can resist various kinds of attack as well. Unfortunately, Li et al. [23] showed that their schemes can't achieve the proper authentication and is suffered from various well known attacks and proposed an improved dynamic ID based remote user authentication scheme in multi server architecture and claimed that, their schemes can resist against all well known attacks and provide the proper authentication, forward secrecy and known key secrecy. But, during our research we found, the proposed scheme is not that much secure as they claimed that is, if the attacker extracts the secret information from the stolen smart card somehow, then adversary can easily guess the correct password PW and real identity ID by eavesdropping any previous login request message, without knowing master secret key x, that is stolen smart card attack and also fails to resist user impersonate attack. Moreover, they have overlooked one of the important features of the smart card that, in the case of lost or stolen smart card there must be some mechanism by which user can invalidate the stolen one and issue a new smart card i.e. smart card revocation phase. To overcome such weaknesses and missing features, we propose a secure and improved anonymous remote user authentication scheme for multi server environments that 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 the Li et al.'s scheme and their flaws respectively. Our improved scheme is presented in section 4. In section 5, we analyze the security mechanism of our proposed scheme and compare the functionality features of our scheme with related schemes in section 6. Lastly, we complete 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 throughout this paper as mentioned by Li et al., which are summarized in Table-1. Here, we will review the existing remote user authentication of Li et al.'s scheme under multi-server environments. Their scheme has four phases, as registration, login, verification and password change phase. We explain the registration, login and verification phases only because we will use them to carry out in the cryptanalysis section. 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:

Before accessing the remote server S_j, the remote user U_i must have to register him/her self to registration center RC. The details of this phase are defined as 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 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) on the smart card and forwards this smart card through a secure channel and finally U_i safely stores b into it.

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 the 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 precedes 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.

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

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 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 computes $Sk= h(D_i||A_i||N_i||N_j||SID_j)$, which is considered as their session key for future secure communication.

3. FLAWS OF LI ET AL.'S SCHEME

Although Li et al. [23] claimed that their scheme is much secure and resists various kind of well known attacks, but we will prove that their scheme in not that much secure as they have claimed and suffers from stolen smart card attack and user impersonate attack, also does not support to revoke the stolen or lost smart card by invalidating the oldest one. The details of our analysis are given as below:

3.1 Stolen Smart Card Attack

In security analysis section, they 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 the master secret key x, as they are protected by one way hash function. However, in this section, we 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 any knowledge of master secret key x. Cryptanalysis steps are given as follows:

i). The attacker Z obtains the secret values $\{C_i, b, D_i, h(y)\}$ from the lost smart card and eavesdrops 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 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 also can guess 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 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 correct one.

From the above analysis we can see that, how the adversary can guess the real identity and password successfully without any knowledge about the master secret key x, but extracting only the secret information from smart card and eavesdropping any previous login request. Because, in modern era due to the speed of computational process is not being limited any more, difficulty of exhaustive searching for such secret information may not survive. Hence, their scheme cannot resist stolen smart card attack.

3.2 User Impersonate Attack

Assume that adversary Z extracts the secret parameters $\{C_i, D_i, E_i, b, h(.), h(y)\}$ from the smart card and eavesdropping 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 creating a forge login message easily to fool a server S_x without knowing PW_i. Where S_x is any service provider sever and can be server S_j too. To perform 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 $P'_{ix} = E_i \oplus h(h(SID_x||h(y))||N_z)$, $CID'_i = A_i \oplus h(D_i||SID_x||N_z)$, $M'_1 = h(P'_{ix}||CID'_{ix}||D_i||N_z)$, $M'_2 = h(SID_x||h(y)) \oplus N_z$, and send $\{ P'_{ix} , CID'_i, M'_1, M'_2\}$ 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 the 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 smart card in some way and eavesdropping any previous login request then adversary Z can easily impersonate as a legal user U_i and share a session key Sk with the server S_x. So Li et al.'s scheme cannot resist such kind of user impersonate 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 [23] that in case if the smart card is lost or stolen by adversary there should have a provision of invalidating the lost or stolen smart card and generate a new one, otherwise an adversary can impersonate as valid registered user, as we have shown 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 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. OUR IMPROVED 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 is 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 given below:

4.1 Registration Phase

This phase is invoked, when a new user U_i wants to access the service from remote servers or reregistering 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 registration center 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 value N=0. Otherwise, if U_i is reregistering then RC increments the value of N by one and stores values of ID_i and N in the database. Then RC computes the following steps as shown 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 into the smart card and it contains $\{B_i, V_i, D_i, E_i, h(y), h(.), b\}$.

These steps complete the registration process of the remote user.

4.2 User Login Phase

This is the phase when the remote users U_i interact with the system by login and want to get 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 succeed, then proceed to next steps, otherwise smart card rejects the login request.

ii). After the verification 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.

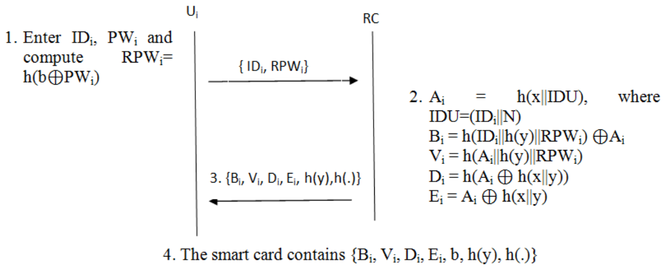


Fig. 1. The registration phase of our scheme

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_i further computes $h(A_i||D_i||CID_i||N_i)$ and compares with received C_1. If does not match, S_i simply rejects the login request and terminates this session. Otherwise, S_j generates a random nonce N_j and computes $C_3 = h(SID_j||D_i||RPW_i||N_j)$, $C_4 = RPW_i \oplus N_i \oplus N_j$ 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 does not match, 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 makes 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 mechanism 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 has to 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 V_i^* and stores V_i in smart card.

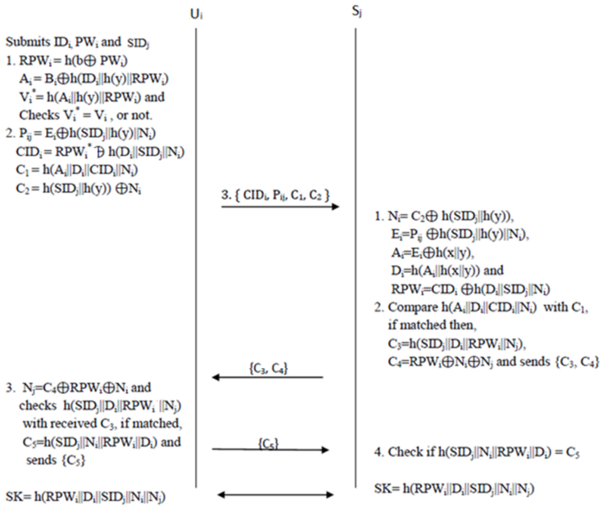


Fig.2. Login, Authentication and session key agreement of proposed scheme

iv). If they are equal, 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. Now, the password is successfully updated.

4.5 Revocation of User's Lost or Stolen Smart Card

During our registration phase, the registration center RC uses to store 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 (eg: by providing his/her first school name, date of birth etc), RC updates the stored credentials incrementing the value of N by 1 and follows the same procedure as done during 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, because of all the parameters of the smart cards has 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 extracts the secret information { B_i, V_i, D_i, E_i, h(y), b, h } from the stolen smart card somehow and eavesdropped any previous login request {CID_i, P_{ij}, C_1, C_2} then also it is infeasible to compute any forge login request that can pass the authentication phase successfully without knowing ID_i andRPW_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 examines all possible passwords 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, neither can create the fake login request nor can guess the correct ID_i and PW_i in the same polynomial time. Therefore, the proposed scheme is secure against stolen smart card attacks.

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 the user U_i or the 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 acknowledge message {C_3, C_4} from the server S_j. However, Z cannot compute {C_5} as a mutual message 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. In the same way, 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 $h(SID_j||D_i||RPW_i||N_j)$ will not be equal to C_3, as because the differences of the two random numbers N_i of these two different sessions, the computed N_j will not be matched with random number N_j of this session which was generated by S_j. Hence, the proposed scheme is secure 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 remote server S_j. To do so, the attacker must be able to create a valid login request {CID_i, P_{ij}, C_1, C_2} to fool S_j. However, it is infeasible to compute a valid forge 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 registered but malicious user then also cannot prove himself as a another legal user, even though with the intercepted login message and his/her smart card, it is just impossible to compute D_i and RPW_i without knowing h(x||y), b and PW_i. Similarly, if any how the attacker gets the valid user's smart card and retrieves the secret information { B_i,V_i, D_i, E_i, h(y), b, h}from it then also the attacker cannot create any forge login request to fool S_j even by eavesdropped any previous login request message { CID_i, P_{ij}, C_1, C_2}. Since, he/she cannot use these parameter to get the correct value of A_i, from extracted value E_i without knowing h(x||y). Therefore, without having the A_i it is impossible to create a 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 registration center can access other server by stealing the identity and password verifier from the registration center verifier table. However, in the proposed scheme, U_i uses to register himself to RC by presenting $RPW_i = h(b \oplus PW_i)$ instead of PW_i and $h(PW_i)$. During the 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 the verifier 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 issue 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 uses to increment 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 with the lost or stolen smart card to login into the system, then cannot prove himself as a valid user, because of changes in registered record database with the new value 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) has 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.

6. PERFORMANCE AND SECURITY COMPARISON

Here, we have compared 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 the Table-2 we can analyze that our scheme provides more security and functional features as compared to other schemes. Because of bitwise XOR and concatenation operation can overhead the computational cost very less, so we have not added these two operations in our account to comparison purpose. We can see from Table-3 that, our scheme has been designed by adding two more hash functions as in Li et al.'s scheme but same as Lee et al.'s scheme, besides our scheme can protect against stolen smart card attack and user impersonate attack and has additional features of smart card revocation too. Hence, our scheme is more secure 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 [22]	Yes	Yes	No	Yes	No	Yes
Our Proposed scheme	Yes	Yes	Yes	Yes	Yes	Yes

Table – 3 Performance comparison with other related schemes

Schemes	Registration Phase	Login Phase	Authentication Phase
X. Li et al.'s [23]	6H	7H	8H
Lee et al.'s [22]	7H	7H	9H
Our Proposed Scheme	7H	7H	9H

7. CONCLUSION AND FUTURE WORK

Due to remote user authentication scheme becomes a great research challenge over an insecure communication network, many schemes have been proposed to provide the higher level of security and with many functional features. Li. et al's proposed a scheme where the remote user can authenticate 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 been proposed. This scheme consists of some more additional features and provides the perfect security against the well known attacks. In future, we try to reduce the computational overhead in terms of less numbers hash functions and message exchange communication without compromising the security issues.

REFERENCES

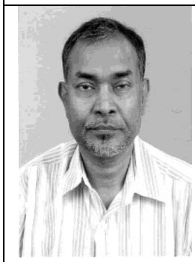
[1] L. Lamport, "Password authentication with insecure communication", Communications of the ACM, Vol. 24(11), pp. 770-772, 1981.
[2] R. E. Lemon, S. M. Matyas, C. H. Meyar, "Cryptographic authentication of time-invariant quantities", IEEE Trans. Communication, Vol. 29, pp. 773-777, 1981.

[3] M. S. Hwang, L. H. Li, "A new remote user authentication scheme using smart cards", IEEE Transaction on Consumer Electronics, vol. 46(1), pp. 28-30, 2000.
[4] E. J. Yoon, E. K. Ryu, K. Y. Yoo, "Further improvement of an efficient password based remote user authentication scheme using smart cards", IEEE Transaction on Consumer Electronics, Vol 50(2), pp-612-614, 2004.
[5] M. L. Das, A. Saxena, V. P. Gulati, "A dynamic ID-based remote user authentication scheme", IEEE Transaction on Consumer Electronics, vol. 50(2), pp. 629-631, 2004.
[6] C. W. Lin, C. S. Tsai, M. S. Hwang, "A new strong password authentication scheme using one-way Hash functions", Journal of Computer and Systems Sciences International, vol. 45(4), pp. 623-626, 2006.
[7] C. S. Bindu, P. Reddy, B. Satyanarayana, "Improved remote user authentication scheme preserving user anonymity", International Journal of Computer Science and Network Security, vol. 83, pp. 62-66, 2008.
[8] L. Fan, J. H. Li, H. W. Zhu, "An enhancement of timestamp-based password authentication scheme", Computer Security, vol. 21(7), pp. 665-667, 2002.
[9] J. J. Shen, C. W. Lin, M. S. Hwang, "Security enhancement for the timestamp-based password authentication using smart cards", Computer Security, vol. 22(7), pp. 591-595, 2003.
[10] C. T. Li, M. S. Hwang, "An efficient biometric based remote user authentication scheme using smart cards", Journal on Networking and Computer Applications, vol. 33, pp. 1-5, 2010.
[11] A. K. Das, "Analysis and improvement on an efficient biometric based remote user authentication scheme using smart cards", IET Information Security, vol. 5(3), pp. 541-552, 2011.
[12] C. H. Lin, Y. Y. Lai, "A flexible biometric remote user authentication scheme", Computer Standards and Interfaces, vol. 27(1), pp.19-23, 2004.
[13] L.H. Li, L.C. Lin, M.S. Hwang, "A remote password authentication scheme for multi-server architecture using neural networks", IEEE Transaction on neural networks, vol. 12, pp. 1498-1504, 2001.
[14] W.S. Jung, "Efficient multi server-password authentication key agreement using smart cards", IEEE Transactions on Consumer Electronics, vol. 50, pp. 251-255, 2004.
[15] M. L. Das, A. Saxena, V.P. Gulati, "A dynamic ID-based remote user authentication scheme", IEEE transactions on Consumer Electronics, Vol. 50,(2), pp. 629-631, 2004.
[16] I. Liao, C.C. Lee, 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'05, Seoul, Korea, pp. 437-440, 2005.
[17] Y.P. Liou, J. Lin, S.S. Wang, "New dynamic ID-based remote user authentication scheme using smart cards", Proceedings of 16th information security conference, Taiwan, pp. 198-205, 2006.
[18] E. J. Yoon, K.Y. Yoo, "Improving the dynamic ID-based remote mutual authentication scheme", Proc. OTM Workshops, LNCS 4277, pp. 499-507, 2006.
[19] Y. Y. Wang, J. Y. Kiu, F. X. Xiao, J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme", Computer Communications, Vol. 32(4), pp. 583-585, 2009.
[20] M. K. Khan, S.K. Kim, K. Alghathbar, "Crypyanalysis and security enhancement of a more efficient and secure dynamic ID-based remote user authentication scheme", Computer Communication, Vol. 34, pp. 305-309, 2011.
[21] C. C. Lee, T. H. Lin, 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(11),pp. 13863-13870, 2011.
[22] R. Madhusudhan, R. C. Mittal, "Dynamic Id-based remote user password authentication schemes using smart cards: A review", journal of network and computer application, vol. 35(4), pp. 1235-1248, 2012.

[23] X. Li, J. Ma, W. Wang, Y. Xiong, J. Zhang, "A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments", Mathematical and computer Modeling, Vol. 58, Issues 1-2, pp. 85-95, 2013.

BIBLIOGRAPHY OF AUTHORS

Subhasish Banerjee 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** received his M.Tech degree in Information Technology from Sikkim Manipal University, Sikkim, India in 2012. Currently, he is 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.
	**Prof. Chandan Tilak Bhunia** 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.