An Efficient and Secure Multi-server Smart Card based Authentication Scheme

Toshi Jain
Department of Computer Science Engineering
Oriental Institute of Science & Technology
Bhopal, India

Sandeep Pratap Singh
Department of Computer Science Engineering
Oriental Institute of Science & Technology
Bhopal, India

ABSTRACT

This paper proposes an efficient and robust multi-server authentication scheme using smart cards. Security of this scheme depends upon cryptographic one-way hash function. This scheme allows remote users to access multiple servers without any need of separately registering with each server. Also, it gets rid of the use of verification table, permits users to select and update the password securely without taking help from the server or registration center, achieves mutual authentication and establishes a session key that is common between user and the server. Moreover, the proposed scheme withstands user impersonation attack, reflection and parallel session attacks, server impersonation attack, replay attack, password guessing attack, smart card loss attack, insider attack, and stolen verifier attack.

General Terms

Security Attacks, Authentication,Cryptography.

Keywords

BAN logic, Hash function, Multi-server, Nonce, Session key, Smart card

1. INTRODUCTION

In today's era, a lot of network services are provided by remote servers. To access these services, conventional remote user authentication is usually a handy means to validate the user's authenticity. Authentication is the fundamental necessity prior to the user avail the server through computer networks as it avoids unauthorized access. In traditional password based authentication schemes, server keeps user identity and password for all the registered users in a verification table. But, there is a risk in such a process; a legal user could be impersonated by an intruder who intercepts the messages from the network and then login to the server later using the intercepted information. Also, if an intruder passes the security of server; the verification table can be easily modified. To handle this problem, one can encode the password using hash function and then store it in a verification table [1]. However, size of the verification table is directly relative to the number of users which means that as the number of users increases, the size of the verification table will get increased. To eliminate such problem, a password authentication scheme based upon smart card has been proposed. Smart card is a tamper resistant integrated circuit card with memory and processor capable of performing computations. In this scheme, server does not maintain a verification table to authenticate the legitimate user.

2. LITERATURE SURVEY

In a single server environment, a server is responsible for offering services to all the authorized remote users. In this direction, many attractive authentication schemes using smart cards have been proposed during the last decade. A remote user authentication scheme based on ElGamal's cryptosystem was proposed [2]. It was claimed that the scheme does not maintain any verification table and it resists replay attack. But, it is exposed to impersonation attack [3]. A dynamic ID-based remote user authentication scheme using one way hash function has been proposed [4]. It was claimed that the scheme allows the users to choose and change their passwords freely, secure against ID-theft, and resists forgery attack, replay attack, guessing attack, stolen verifier attack and insider attack. However, it was proved that the scheme is insecure against guessing attack and does not provide mutual authentication [5]. To defeat these flaws, a new scheme was also suggested which was then cryptanalyzed through impersonation attack and proposed an improved scheme [6]. Major drawbacks in this scheme are a) It does not provide secure password change phase b) User has to remember the secret number Y_i.

Song [7] proposed a smart card authentication scheme based on symmetric key cryptography and claimed that the scheme is able to resist the existing potential attacks. In addition, it provides mutual authentication and shared session key. Nevertheless, Song's scheme fails to provide early wrong password detection and perfect forward secrecy.

If a user wishes to access several network services, he or she has to register with different servers and maintain different corresponding user IDs and PWs. To overcome this difficulty, several schemes have been proposed. These authentication schemes enable users to obtain service from multiple servers without separately registering with each server. In this context, multi-server authentication scheme using neural networks has been proposed [8]. In this, users can freely choose their passwords. The major drawback of this approach is that it spends long time on training neural networks [9]. To overcome the weakness of time synchronization, a nonce based scheme using one-way hash function and symmetric cryptosystem was proposed [10]. It has all the previous advantages as well as server and user authenticate each other and generate a session key agreed between them. Though, it is weak against insider attack and fails to provide forward secrecy [11].

A dynamic ID based remote user authentication scheme has been given to provide user anonymity using one way hash function [12]. It has been proved that the scheme fails to provide forward secrecy [13]. It has been pointed out that the scheme [12] does not resist impersonation attack, insider attack, registration centre spoofing attack, server spoofing attack, fails to provide mutual authentication and further improvement has been proposed [14]. Though, Sood et al. [15] showed that Hsiang-Shih's improved scheme fails to provide security against impersonation attack, replay attack, stolen smart card attack and has incorrect password change phase. Tsai [16] offered a nonce based scheme using one way hash function. However, Zhu [17] proved that Tsai's scheme is susceptible to server spoofing attack and fails to provide perfect forward secrecy. To overcome these drawbacks, they proposed an improved scheme also. Tseng et al. [18] proposed an efficient pairing-based user authentication scheme with smart cards. However, in 2013, Liao and Hsiao [19] indicates that Tseng et al.'s scheme is exposed to offline dictionary attack, insider attack, malicious server attack and cannot provide proper mutual authentication and session key agreement. Wang and Ma [20] proposed smart card based efficient and secured multi- server authentication scheme. Its security relies on the difficulty of solving Elliptic Curve Discrete Logarithm Problem (ECDLP). The authors claimed that their scheme is able to resist replay attack, offline dictionary attack and server spoofing and impersonation attack. But, it shows inadequacy to provide security against server spoofing attack, the impersonation attack, the privileged insider attack and the offline password guessing attack [21]. Besides, it is mentioned that the scheme eliminates use of verification table as only certain secret keys are stored in user's smart card, servers and RC. However, without storing ID of users there is no way to identify correct secret key of a particular user. It means that each server stores every registered user's information in a verification table. Moreover, it fails to provide early wrong password detection. In addition, it possesses inefficient password change phase due to the involvement of RC which makes it time consuming. Chen et al. [22] also proposed their scheme but involvement of RC during verification makes it inefficient practically.

Based on these inspirations, this paper presents secure multi-server authentication scheme using smart cards. Breaking this scheme is as complex as solving the cryptographic one-way hash function. This scheme allows remote users to access multiple servers without any need of separate registration. It eliminates the need of verification table, permits users to choose and update the password securely, provides mutual authentication session key generation. Additionally, it offers security against server impersonation attack, user impersonation attack, reflection and parallel session attacks, replay attack, insider attack, password guessing attack, stolen verifier attack and smart card loss attack. Thus, the proposed scheme is really appropriate in distributed multi-server environment such as the Internet.

3. PROPOSED SCHEME

This section describes the proposed smart card authentication scheme. Suppose, there are a total of n servers and the new user wants to communicate with these servers. Every user and server has to register initially with the registration center. The notations that are used throughout this paper summarized in Table 1.

Table 1. Notations Used

Symbols	Their Meaning
RC	registration center
U_i	i^{th} remote user
ID_i	identity of U_i
PW_i	password chosen by U_i
PW_i^*	password guessed by the adversary
S_j	j^{th} authentication server $(1 \le j \le n)$
SID_j	identity of S_j
x	secret key of RC
d	secret number of RC
$h(\bullet)$	cryptographic one way hash function
$\oplus$	bitwise XOR operation
$SKey_{ij}$	session key shared between U_i and S_j
N_1	random nonce generated by U_i
N_2	random nonce generated by S_j
- - - - - ▶	secure channel
⟶	insecure channel

The scheme consists of four phases: Registration phase, Login phase, Authentication phase and Password Change phase.

3.1 Registration Phase

This phase is divided into two sub-phases: Server Registration phase and User Registration phase (as shown in Fig. 1).

3.1.1 Server registration phase: In this phase, S_j selects SID_j and submits it to RC over a secure channel. Upon receiving the registration request from S_j, RC computes the server secret parameter $SS_j = h(SID_j, h(x)) \oplus h(d)$ and sends $\{SS_j, h(d)\}$ *to* S_j through a secure channel.

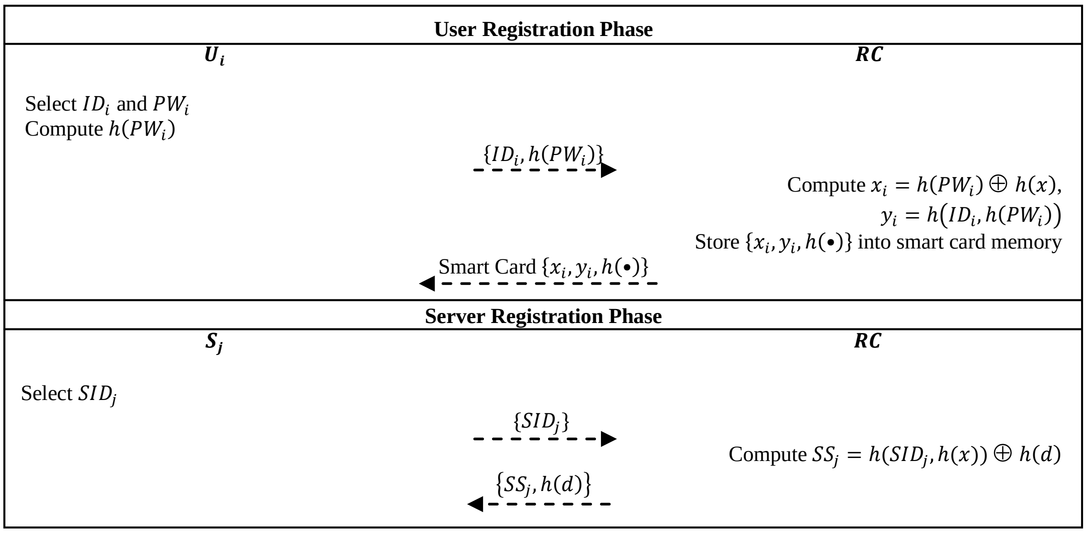

User Registration Phase
U_i
RC
Select ID_i and PW_i
Compute $h(PW_i)$
$\{ID_i, h(PW_i)\}$
Compute $x_i = h(PW_i) \oplus h(x)$,
$y_i = h(ID_i, h(PW_i))$
Store $\{x_i, y_i, h(\bullet)\}$ into smart card memory
Smart Card $\{x_i, y_i, h(\bullet)\}$
Server Registration Phase
S_j
RC
Select SID_j
$\{SID_j\}$
Compute $SS_j = h(SID_j, h(x)) \oplus h(d)$
$\{SS_j, h(d)\}$

Fig 1: User and Server registration phase

3.1.2 User registration phase: U_i selects ID_i and PW_i, computes $h(PW_i)$ and submits $\{ID_i, h(PW_i)\}$ to RC over a secure channel. Once the registration request is received, RC computes $x_i = h(PW_i) \oplus h(x)$, $y_i = h(ID_i, h(PW_i))$ and issues a smart card over secure channel to U_i by storing $\{x_i, y_i, h(\bullet)\}$ into smart card memory.

3.2 Login Phase

The login and authentication phases are shown in Fig. 2. In this phase, U_i inserts the smart card to the card reader and keys in ID_i and $PW_i^{'}$. The smart card computes $y_i^{'} = h\left(ID_i, h(PW_i^{'})\right)$ and verifies whether computed $y_i^{'}$ equals stored y_i or not. If not, user is not the genuine owner of smart card. If true, reader generates a random nonce N_1, computes $a_i = x_i \oplus h(PW_i)$, $b_i = h(SID_j, a_i)$, $c_i = h(b_i, N_1)$, $\{ID_i, SID_j, N_1, c_i\}$ and sends the login request $\{ID_i, SID_j, N_1, c_i\}$ to S_j.

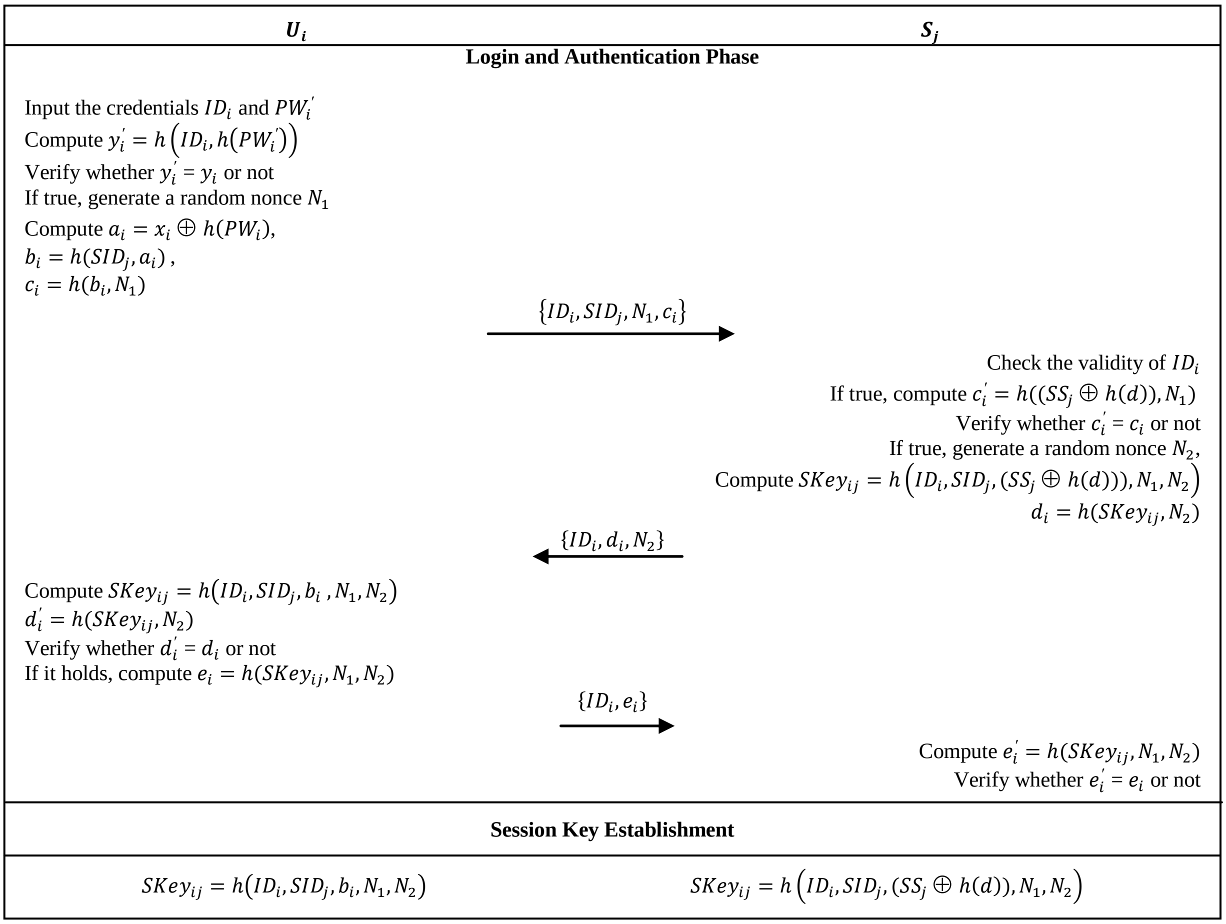
3.3 Authentication Phase

Upon receiving the login request $\{ID_i, SID_j, N_1, c_i\}$; S_j first checks the validity of ID_i to accept/reject the login request. If true, S_j computes $c_i^{'} = h\left(\left(SS_j \oplus h(d)\right), N_1\right)$ and then checks whether computed c_i' equals received c_i or not. If it holds, S_j generates a nonce N_2, computes the $SKey_{ij} = h(ID_i, SID_j, (SS_j \oplus h(d)), N_1, N_2)$, $d_i = h(SKey_{ij}, N_2)$ and sends the message $\{ID_i, d_i, N_2\}$ to U_i.

After getting the message $\{ID_i, d_i, N_2\}$ from S_j, U_i computes $SKey_{ij} = h(ID_i, SID_j, b_i, N_1, N_2)$, and $d_i^{'} = h(SKey_{ij}, N_2)$ and checks whether the computed $d_i^{'}$ equals received d_i or not. If it holds, S_j is authentic otherwise terminate the session. Subsequently, U_i computes $e_i = h(SKey_{ij}, N_1, N_2)$ and sends $\{ID_i, e_i\}$ to S_j. Once the message $\{ID_i, e_i\}$ is received, S_j computes $e_i^{'} = h(SKey_{ij}, N_1, N_2)$ and checks whether computed $e_i^{'}$ equals received e_i or not. If it holds, mutual authentication is achieved. Both the parties agree upon a common shared session key $SKey_{ij} = h(ID_i, SID_j, b_i, N_1, N_2) = h(ID_i, SID_j, (SS_j \oplus h(d)), N_1, N_2)$.

3.4 Password Change Phase

This phase is invoked whenever U_i wants to update his or her password. In this phase, U_i inserts the smart card to the card reader and keys in ID_i and $PW_i^{'}$. After this, the smart card computes $y_i^{'} = h\left(ID_i, h(PW_i^{'})\right)$ and verifies whether computed $y_i^{'}$ equals stored y_i or not. If true, U_i enters a new password PW_{inew}. The smart card computes $x_{inew} = x_i \oplus h(PW_i) \oplus h(PW_{inew})$, $y_{inew} = h(ID_i, h(PW_{inew}))$ and stores x_{inew}, y_{inew} instead of x_i, y_i respectively in the smart card memory. Thus, U_i can update the password without taking any assistance from S_j.



U_i **S_j**

Login and Authentication Phase

Input the credentials ID_i and $PW_i^{'}$
Compute $y_i^{'} = h\left(ID_i, h(PW_i^{'})\right)$
Verify whether $y_i^{'} = y_i$ or not
If true, generate a random nonce N_1
Compute $a_i = x_i \oplus h(PW_i)$,
$b_i = h(SID_j, a_i)$,
$c_i = h(b_i, N_1)$

$\xrightarrow{\{ID_i, SID_j, N_1, c_i\}}$

Check the validity of ID_i
If true, compute $c_i^{'} = h((SS_j \oplus h(d)), N_1)$
Verify whether $c_i^{'} = c_i$ or not
If true, generate a random nonce N_2,
Compute $SKey_{ij} = h\left(ID_i, SID_j, (SS_j \oplus h(d))), N_1, N_2\right)$
$d_i = h(SKey_{ij}, N_2)$

$\xleftarrow{\{ID_i, d_i, N_2\}}$

Compute $SKey_{ij} = h(ID_i, SID_j, b_i , N_1, N_2)$
$d_i^{'} = h(SKey_{ij}, N_2)$
Verify whether $d_i^{'} = d_i$ or not
If it holds, compute $e_i = h(SKey_{ij}, N_1, N_2)$

$\xrightarrow{\{ID_i, e_i\}}$

Compute $e_i^{'} = h(SKey_{ij}, N_1, N_2)$
Verify whether $e_i^{'} = e_i$ or not

Session Key Establishment

$SKey_{ij} = h(ID_i, SID_j, b_i, N_1, N_2)$ $SKey_{ij} = h\left(ID_i, SID_j, (SS_j \oplus h(d)), N_1, N_2\right)$

Fig 2: Login and authentication phase

4 FORMAL AUTHENTICATION PROOF BASED ON BAN LOGIC

Mutual authentication and session key establishment must be achieved by an ideal authentication scheme. Burrows et al. [23] proposed the logical analysis which is a useful model to prove the validity of authentication schemes. In this section, BAN logic is used to demonstrate the execution of the proposed scheme.

According to the analytic procedure of BAN logic, the verification goals of this scheme are listed as follows:

$U_i$believes $U_i \overset{SK}{\leftrightarrow} S_j$ $\{G.1\}$

$U_i$believes S_j believes $U_i \overset{SK}{\leftrightarrow} S_j$ $\{G.2\}$

$S_j$believes $U_i \overset{SK}{\leftrightarrow} S_j$ $\{G.3\}$

$S_j$believes U_i believes $U_i \overset{SK}{\leftrightarrow} S_j$ $\{G.4\}$

Now, the scheme is arranged from the generic type to the idealized form as follows:

m1. $U_i \rightarrow S_j : \langle c_i, N_1 \rangle_{\mathrm{h(x)}}$

m2. $S_j \rightarrow U_i : \left(\langle U_i \xleftrightarrow{SK_{ey(i,j)}} S_j, N_1, N_2 \rangle_{\mathrm{h(x)}}, \langle \mathrm{d_i}, \mathrm{N_2} \rangle_{\mathrm{SK_{ey_{i,j}}}} \right)$

m3. $U_i \rightarrow S_j : \langle U_i \xleftrightarrow{SK_{ey_{i,j}}} S_j \rangle_{\mathrm{SK_{ey_{i,j}}}}$

Without loss of generality, following assumptions are made to further analyze the proposed scheme by BAN logic:

U_i believes fresh N_1 $\{A.1\}$

S_j believes fresh N_2 $\{A.2\}$

U_i believes (S_j controls N_2) $\{A.3\}$

S_j believes (U_i controls N_1) $\{A.4\}$

U_i believes $S_j \xleftrightarrow{h(x)} RC$ $\{A.5\}$

S_j believes $U_i \xleftrightarrow{h(x)} RC$ $\{A.6\}$

U_i believes$S_j$believes $S_j \xleftrightarrow{h(x)} RC$ $\{A.7\}$

S_j believes U_i believes $S_j \xleftrightarrow{h(x)} RC$ $\{A.8\}$

Assumptions $\{A.1\}$ and $\{A.2\}$ state that U_i and S_j generate two fresh random nonces N_1 and N_2 and assure their freshness. Assumption $\{A.3\}$ states that U_i believes S_j has jurisdiction right over N_2. Assumption $\{A.4\}$ states that $\mathrm{S_j}$ believes U_i has jurisdiction right over N_1. Assumptions $\{A.5\}$, $\{A.6\}$, $\{A.7\}$ and $\{A.8\}$ have to be revealed in a multi-server environment.

Based on the above-mentioned assumptions and the rules of BAN logic, the main steps of proof are as follows:

By $\mathrm{m_1}$ and seeing rule,

S_j sees $\langle c_i, N_1 \rangle_{h(x)}$ $\{S.1\}$

By $\{A.6\}$, $\{S.1\}$and message meaning rule,

S_j believes U_i said $\langle c_i, N_1 \rangle$. $\{S.2\}$

By $\{A.1\}$, $\{S.2\}$and nonce verification rule,

S_j believes U_i believes c_i. $\{S.3\}$

By $\{A.4\}$, $\{S.3\}$and jurisdiction rule,

S_j believes c_i. $\{S.4\}$

By $\mathrm{m_2}$ and seeing rule,

U_i sees $\left(\langle U_i \xleftrightarrow{SK_{ey(i,j)}} S_j, N_1, N_2 \rangle_{\mathrm{h(x)}}, \mathrm{C} \right)$. $\{S.5\}$

By $\{S.5\}$ and breaking the conjunction,

U_i sees$\left(\langle U_i \xleftrightarrow{SK_{ey(i,j)}} S_j, N_1, N_2 \rangle_{\mathrm{h(x)}} \right)$ $\{S.6\}$

and

U_i sees$\left(\langle U_i \xleftrightarrow{SK_{ey(i,j)}} S_j, N_1, N_2 \rangle_{\mathrm{h(x)}} \right)$ $\{S.7\}$

By $\{A.5\}$, $\{S.6\}$and message meaning rule,

U_i believes S_j said $\langle U_i \xleftrightarrow{SK_{ey(i,j)}} S_j, N_1, N_2 \rangle$. $\{S.8\}$

By {A.1}, $\{A.2\}$, $\{A.3\}$, $\{S.8\}$ and nonce verification rule,

U_i believes S_j believes$\langle U_i \xleftrightarrow{SK_{ey(i,j)}} S_j \rangle$ $\{S.9\}$

By $\{S.9\}$ and jurisdiction rule,

U_i believes $U_i \xleftrightarrow{SK_{ey(i,j)}} S_j$ $\{S.10\}$

By $\mathrm{m_3}$ and seeing rule,

S_j sees $\langle U_i \xleftrightarrow{SK_{ey_{i,j}}} S_j \rangle_{\mathrm{SK_{ey_{i,j}}}}$ $\{S.11\}$

By $\{A.6\}$, $\{S.11\}$ and message meaning rule,

S_j believes U_i said $U_i \xleftrightarrow{SK_{ey(i,j)}} S_j$ $\{S.12\}$

By ($\{A.4\}$, $\{S.12\}$and nonce verification rule,

S_j believes U_i believes $U_i \xleftrightarrow{SK_{ey(i,j)}} S_j$ $\{S.13\}$

By $\{S.13\}$ and jurisdiction rule,

S_j believes $U_i \xleftrightarrow{SK_{ey(i,j)}} S_j$ $\{S.14\}$

The statements $\{S.9\}$, $\{S.10\}$, $\{S.13\}$ and $\{S.14\}$ together achieve the verification goals $\{G.1\}$, $\{G.2\}$, $\{G.3\}$and $\{G.4\}$ of the proposed scheme. Based on these statements, it is shown that the proposed scheme establishes a secure session key between U_i and S_j. Moreover, both U_i and S_j are able to authenticate each other using this scheme.

5. ANALYSIS ON SECURITY ATTACKS AND USER NEEDED FEATURES

This section demonstrates the proof of correctness of the proposed authentication scheme on the basis of following possible attacks and user needed features.

5.1 User Impersonation Attack

In this proposed scheme, the login request contains $\{ID_i, SID_j, N_1, c_i\}$. It contains $c_i = h(b_i, N_1) = h(h(SID_j, a_i), N_1) = h(h(SID_j, x_i \oplus h(PW_i)), N_1)$. In order to securely perform impersonation attack, the attacker needs to guess the correct values of $h(PW_i)$ and $h(x)$.

5.2 Server Impersonation Attack

It is not possible for an adversary to masquerade as a legitimate server and try to cheat an authentic user because the server response message $\{ID_i, d_i, N_2\}$ is prepared by using the secret parameter $(SS_j \oplus h(d))$ which can be computed by S_j only. Hence, the proposed authentication scheme prevents server spoofing.

5.3 Replay Attack

Here, the replay attack will fail because the freshness of the messages transmitted in the login and authentication phases is provided by the random nonces N_1 and N_2. These are generated independently, and their values differ among sessions. So attackers cannot enter the system by resending the earlier transmitted messages to pretend to be legal users.

5.4 Reflection and Parallel Session Attack

The reflection and parallel session attacks are possible due to the transmission of similar messages. To resist reflection and parallel session attacks, the given scheme employs asymmetric structure of communicating messages, i.e., $\{ID_i, SID_j, N_1, c_i\}$, $\{ID_i, d_i, N_2\}$ and $\{ID_i, e_i\}$. There is no symmetry in the values of $c_i = h(b_i, N_1)$, $d_i = h(SKey_{ij}, N_2)$ and $e_i = h(SKey_{ij}, N_1, N_2)$. Hence, attacker is unable to launch parallel session attack by replaying server response message as the user login request or reflection attack by resending user login request as the server response message.

5.5 Password Guessing Attack

In the proposed scheme, $h(PW_i)$ is not used directly in any of the communicating parameters. Therefore, the scheme is secure against password guessing attack.

5.6 Insider Attack

Since, U_i registers to RC by presenting $h(PW_i)$ instead of PW_i, the insider of RC cannot directly obtain U_i's password PW_i because of the property of one-way hash function. Hence, the proposed scheme is able to resist insider attack.

5.7 Security of the Session Key

In this proposed multi-server authentication scheme, the session key $SKey_{ij} = h\left(ID_i, SID_j, b_i, N_1, N_2\right) = h\left(ID_i, SID_j, (SS_j \oplus h(d)), N_1, N_2\right)$ is associated with $h(PW_i)$, $h(x)$ and $h(d)$ which are unknown to the adversary. Even though the past session key is compromised, the adversary cannot extract these parameters due to the security of one-way hash function. Moreover, it is infeasible to guess these values simultaneously. Thus, the adversary cannot obtain any further session key.

5.8 Smart Card Loss Attack

In the proposed scheme, if U_i's smart card is lost or stolen, it is difficult for any attacker to derive or change the password PW_i. Also, nobody can impersonate the smart card owner to login into S_j without knowing the correct ID_i and PW_i of U_i.

5.9 Stolen Verifier Attack

As the servers and the registration center do not maintain any verification table, the proposed authentication scheme is secure against stolen-verifier attack.

5.10 Single Registration

This scheme allows a valid user to register once and then the user can access all the registered servers.

5.11 No Verification Table

In the proposed scheme, instead of storing passwords of all the registered users in the verification table, server keeps secret key 'x' and secret number 'd' to avoid maintaining verification table used to verify the login request. Hence, the scheme is secure against stolen verifier attack as none of the registered servers need to maintain a verification table.

5.12 User can choose and update the password securely without taking any support from the server or RC

In the scheme, a valid user can the password freely and securely without any assistance from the servers or registration center. As the card reader verifies the old password first in the password change phase, unauthorized users cannot change the authorized user's password even if they get the corresponding smart card.

5.13 Early Wrong Password Detection

If the user U_i inputs a wrong password by mistake, this password will be quickly detected by the card reader itself since reader compares $y_i' = h\left(ID_i, h\left(PW_i'\right)\right)$ with the stored y_i during the login phase. Hence, the scheme provides early wrong password detection.

5.14 Each server uses unique secret parameter

In the scheme, each server has unique secret parameter $SS_j = h(SID_j, h(x)) \oplus h(d)$ used to authenticate the user. Hence, there is no need to store the secret parameter of all the servers in the smart card memory.

5.15 Mutual authentication and session key agreement without the support of RC

This scheme allows valid users and valid servers to authenticate each other and then agree on a session key without any support from the registration center. The generated session key $SKey_{ij} = h\left(ID_i, SID_j, b_i, N_1, N_2\right) = h\left(ID_i, SID_j, (SS_j \oplus h(d)), N_1, N_2\right)$ will be different for each login session.

5.16 The scheme solves time synchronization problem

The proposed scheme uses randomly generated nonces N_1 and N_2 instead of timestamps to avoid time synchronization problem.

6. PERFORMANCE COMPARISON

This section describes comparison among various multi-server authentication schemes with this proposed scheme on the basis of security features as well as possible attacks. Table 2 shows comparative results in terms of security attacks and essential features needed by the users. Here,

F1 = Free from maintaining verification table
F2 = User is allowed to choose the password
F3 = User is allowed to change the password
F4 = Free from involvement of RC/server during password change phase
F5 = Provides mutual authentication
F6 = Provides early wrong password detection
F7 = Provides mutual authentication without support of RC
F8 = Provides session key agreement
F9 = Resists user impersonation attack
F10 = Resists server spoofing attack
F11 = Resists replay attack
F12 = Resists password guessing attack
F13 = Resists reflection attack
F14 = Resists parallel session attack
F15 = Resists known session key attack

Table 2. Comparison among various Multi-server Authentication Schemes with this Proposed Scheme

Security Features	Juang [10]	Liao-Wang [12]	Hsiang-Shih [14]	Sood et al. [15]	Proposed Scheme
F1	No	Yes	Yes	No	Yes
F2	Yes	Yes	Yes	Yes	Yes
F3	No	Yes	Yes	Yes	Yes
F4	Yes	Yes	Yes	Yes	Yes
F5	Yes	Yes	Yes	Yes	Yes
F6	No	Yes	Yes	Yes	Yes
F7	Yes	Yes	No	No	Yes
F8	Yes	Yes	Yes	Yes	Yes
F9	Yes	No	No	Yes	Yes
F10	Yes	No	No	Yes	Yes
F11	Yes	Yes	No	Yes	Yes
F12	Yes	Yes	No	Yes	Yes
F13	Yes	Yes	Yes	Yes	Yes
F14	Yes	Yes	Yes	Yes	Yes
F15	Yes	Yes	Yes	Yes	Yes

Table 3 explores comparative analysis of the proposed scheme with various smart card authentication schemes under multi-server environment. Meaning of notations used in the tables is defined as follows:

H = One Way Hash Function
En = Symmetric Encryption
De = Symmetric Decryption

Table 3. Comparison of the Proposed Scheme in terms of Computational Complexity

Schemes	Registration Phase	Login and Authentication Phase	Total
Juang [10]	3H + 1En	5H + 3En + 4De	**8H + 4En + 4De**
Liao-Wang [12]	5H	16H	**21H**
Hsiang-Shih [14]	7H	23H	**30H**
Sood et al. [15]	5H	25H	**30H**
Proposed Scheme	5H	11H	**16H**

7. CONCLUSION

It is clear from this table that this proposed scheme is computationally efficient as well as secure compare to existing authentication schemes. This paper portraits an efficient and secure smart card authentication scheme for multi-server architecture. It is shown that the proposed scheme satisfies all of the essential security requirements as it is safe against user and server impersonation attacks, replay attack, reflection and parallel session attacks, password guessing attack, stolen verifier attack, smart card loss attack and insider attack. The other qualities comprises:

- It doesn't need verification table.
- It allows users to choose and change their passwords freely without taking any assistance from the server or registration center.
- It permits users to access multiple servers without separately registering with each server.
- It detects wrong password early, provides mutual authentication and session key agreement.
- It avoids the time-synchronization problem.

8. ACKNOWLEDGMENT

The author wants to thank Prof. Sanjay Sharma for his kind support. Discussions with him greatly inspired the author for some worthful comments.

9. REFERENCES

[1] L. Lamport, 1981 "Password authentication with insecure communication", Communications of the ACM, vol. 24, no.11, , pp. 770-772.

[2] M.S. Hwang and L.H. Li, 2000 "A new remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, vol. 46, no. 1, pp. 28-30.

[3] C. K. Chan and L. M. Cheng, 2000 "Cryptanalysis of a remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, vol. 46, no. 4, pp. 992-993.

[4] Manik Lal Das, Ashutosh Saxena, and Ved P. Gulati, 2004 "A dynamic ID-based remote user authentication scheme", IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 629-631.

[5] I-En Liao, Cheng-Chi Lee and Min-Shiang Hwang, 2005 "Security enhancement for a dynamic ID-based remote user authentication scheme", International Conference on Next Generation Web Services Practices.

[6] Qi Xie, Ji-Lin Wang, De-Ren Chen and Xiu-Yuan Yu, 2008 "A novel user authentication scheme using smart cards", International Conference on Computer Science and Software Engineering, , pp. 834-836.

[7] R. Song, 2010 "Advanced smart card based password authentication protocol," Computer Standards & Interfaces, vol. 32, no. 5-6, , pp. 321-325.

[8] L. Li, I. Lin and M. Hwang, 2001 "A Remote Password Authentication Scheme for Multi-server Architecture Using Neural Networks," IEEE Trans. on Neural Networks, vol. 12, no. 6, pp. 1498-1504.

[9] I.C. Lin, M.S. Hwang and L.H. Li, 2003 "A new remote user authentication scheme for multi-server architecture", Future Generation Computer Systems, vol. 19, no. 1,, pp. 13-22.

[10] W.S. Juang, 2004 "Efficient multi-server password authenticated key agreement using smart cards", IEEE Transactions on Consumer Electronics, vol. 50, no. 1, pp. 251-255.

[11] Wei-Chi Ku, Hsiu-Mei Chuang, Min-Hung Chiang and Kuo-Tsai Chang, 2005 "Weaknesses of a multi-server password authenticated key agreement scheme", 2005 National computer Symposium, pp. 1-5.

[12] Y.P. Liao and S.S. Wang, 2009 “A secure dynamic ID based remote user authentication scheme for multi-server environment”, Computer Standards & Interfaces, vol. 31, no. 1, pp. 24-29.

[13] Te-Yu Chen, Min-Shiang Hwang, Cheng-Chi Lee, Jinn-Ke Jan, 2009 “Cryptanalysis of a secure dynamic ID based remote user authentication scheme for multi-server environment,” 2009 Fourth International Conference on Innovative Computing, Information and Control, pp. 725-728.

[14] Cheng Hsiang and Wei-Kuan Shih, 2009 “Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment”, Computer Standards & Interfaces, vol. 31, no. 6, , pp. 1118-1123.

[15] Sandeep K. Sood, Anil K. Sarje and Kuldip Singh, 2011 “A secure dynamic identity based authentication protocol for multi-server architecture”, Journal of Network and Computer Applications, vol. 34, no. 2, , pp. 609-618.

[16] J.L. Tsai, 2008 “Efficient multi-server authentication scheme based on one-way hash function without verification table”, Computers & Security, vol. 27, no. 3-4, pp.115-121.

[17] Hongfeng Zhu, Tianhua Liu and Jie Liu, 2009 “Robust and simple multi-server authentication protocol without verification table”, Ninth International Conference on Hybrid Intelligent Systems, 2009, pp. 51-56.

[18] Y. M. Tseng, T. Y. Wu, J. D. Wu, 2008 “A pairing-based user authentication scheme for wireless clients with smart card,” Informatics, vol. 19, no. 2, pp. 285-302.

[19] Yi-Pin Liao, Chih-Ming Hsiao, 2013 “A novel multi-server remote user authentication scheme using self-certified public keys for mobile clients, Future Generation Computer Systems, vol. 29, pp. 886-900.

[20] B. Wang and M. Ma, “A smart card based efficient and secured multi-server authentication scheme," Wireless Personal Communications, vol. 68, 2013, pp. 361-378.

[21] D. He and S. Wu, “Security flaws in a smart card based authentication scheme for multi-server environment," Wireless Personal Communications, 2013.

[22] T. Y. Chen, C. C. Lee, M. S. Hwang and J. K. Jan, “Towards secure and efficient user authentication scheme using smart card for multi-server environments," Wireless Personal Communications, vol. 66, 2013, pp. 1008-1032.

[23] Michael Burrows, 1990 Martin Abadi and Roger Needham, “A logic of authentication,” ACM Transactions on Computer Systems, vol. 8, no. 1, pp. 18-36.