ENHANCED MULTI-SERVER SMART CARD AUTHENTICATION SCHEME

Priyanka Sinha[1] and Akhilesh Bansiya[2]
Department of Computer Science & Engineering
Vedica Institute of Technology
RKDF University, Bhopal

Corresponding Author: Priyanka Sinha Manuscript Received: Manuscript Accepted:

Abstract
A robust multi-server smart card authentication scheme has been proposed by Tyagi et al. using cryptographic one-way hash function and the discrete logarithm problem. However, it has been observed that the scheme proposed by Tyagi et al. is susceptible to impersonation attack. In the present paper, an improved smart card based password authentication scheme is proposed based on one way hash function.

I. INTRODUCTION

Since last few years, electronic transactions carried out over the Internet are gaining popularity and are widely accepted in the world. To keep data secure during its transmission over insecure network, sufficient security measures are needed. One of the imperative key factors in security is authentication which is required for every transaction. It is the basic requirement prior to allow the user accesses the server. A lot of work has been done to secure the information from unauthorized access [1, 2]. One among various authentication schemes is password supported authentication scheme. In conventional password supported authentication schemes, server keeps verification table securely to verify the authenticity of a user. Every user has its own credentials, identifier (ID) and password (PW). Whenever a user desires to access resources from a server, he/she has to present ID and PW to pass the authentication phase. The server verifies the PW corresponding to the ID from verification table and authenticates the user if the submitted password matches with the stored password.

However, this technique is insecure since an attacker can access the contents of the verification table to break down the entire system. Storing the password in hashed format is one of the solutions [3]. The major drawback in this approach is the verification table size which is directly relative to the number of users; as a result security risk on the server increases. To resist potential attacks on the verification tables, smart card based password authentication scheme has

been suggested [4]. In this authentication scheme, server needs not to preserve any verification table. It maintains only its own long term secret key(s).

Smart cards are similar to shape and size of credit cards embedded with microprocessors capable of holding important information of the person who holds them. They are safer than magnetic strip cards. Smart card provides authentication and identification for the users. Smart cards are widely accepted in Europe for the healthcare sector, compared to the rest of the world. In fact, Europe is the biggest consumer of smart card technology in the world and healthcare is the third-largest sector in the world to deploy smart cards, behind pay phones and Global System for Mobile Communications (GSM) applications. It has been suggested that a minimum level of security should be provided by the current European smart card legislation. To achieve this, a secure secret key storage is required. Smart cards are the perfect option to offer the necessary level of security.

Since last two decades, various smart card based authentication schemes have been proposed [5–7, 9, 10, 12–17]. To overcome the weaknesses in multi-server environment, a nonce based scheme using one-way hash function and symmetric cryptosystem was proposed [18]. It has all the previous advantages as well as server and user authenticate each other and generate a session key agreed between them. Nevertheless, it demonstrates insider attack and does not offer forward secrecy [19]. Further improvement was also proposed [20]. They claimed that their scheme provides mutual authentication between the remote server and the user, resists server spoofing attack, stolen-verified attack, replay attack, smart card loss attack and achieves forward secrecy.

A dynamic ID based remote user authentication scheme has been given to provide user anonymity using one way hash function [21]. It has been proved that the scheme fails to provide forward secrecy [22]. It has been pointed out that the scheme [21] does not oppose insider attack, server spoofing attack, impersonation attack, registration centre spoofing attack, not succeeds to afford mutual authentication and further improvement has been proposed [23]. Though, Sood et al. [24] showed that Hsiang-Shih's improved scheme fails to provide security against replay attack, impersonation attack, stolen smart card attack and has incorrect password change phase.

Contribution of this Paper :

In 2012, Tyagi suggested robust multi-server authentication scheme using smart cards [25]. Its security is based on cryptographic one-way hash function and the discrete logarithm problem. This scheme permits remote users to access multiple servers while not singly registering with every server. Moreover, it eliminates the employment of verification table, permits users to settle on and alter the firmly while not taking any help from the server or registration center, provides mutual

authentication and establishes a typical session key between user and the server. To boot, the proposed scheme withstands all the potential attacks. To overcome the weaknesses present in Tyagi et al.'s scheme, this paper proposes an improved scheme using one way hash function.

The rest of the paper is structured as follows. Section II shows improved scheme and its security analysis is explained in section III. Section IV presents performance comparison and at last, conclusion has been given by section V.

II. PROPOSED IMPROVED SMART CARD AUTHENTICATION SCHEME

This section describes the proposed smart card authentication scheme. The scheme consists of four phases: Registration, Login, Authentication and Password Change phase.

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 $(1 \leq j \leq n)$
SID_j	identity of S_j
x	secret key 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_u	random nonce generated by U_i
N_s	random nonce generated by S_j
$\|\|$	message concatenation
------►	secure channel
——►	insecure channel

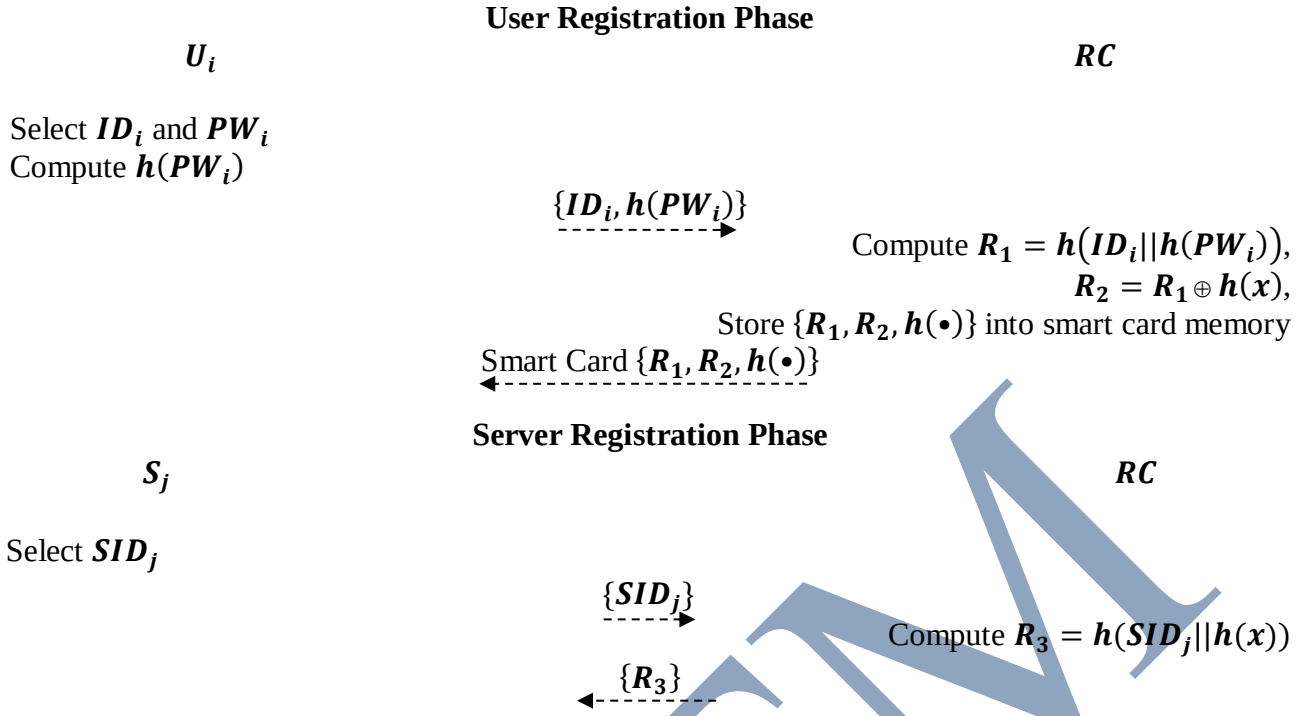

Figure 1. Proposed registration phase

Registration Phase :

This phase is divided into two sub-phases: Server Registration phase and User Registration phase (as shown in Figure 1). Before going through these phases in detail, let us know that *RC* initially computes $h(x)$ in advance.

Server registration phase: In this phase, $\boldsymbol{S_j}$ selects $\boldsymbol{SID_j}$ and submits it to $\boldsymbol{RC}$ over a secure channel. Upon getting the registration request from $\boldsymbol{S_j}$, $\boldsymbol{RC}$ computes the server secret parameter $\boldsymbol{R_3} = \boldsymbol{h(SID_j||h(x))}$ and sends $\{\boldsymbol{R_3}\}$ to $\boldsymbol{S_j}$ through a secure channel.

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 $R_1 = h(ID_i||h(PW_i))$, $R_2 = R_1 \oplus h(x)$ and issues a smart card over secure channel to U_i by storing $\{R_1, R_2, h(\bullet)\}$ into smart card memory.

Login Phase :

The login and authentication phases are shown in Figure 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 $R_1 = h(ID_i||h(PW_i))$ and verifies whether computed R_1 equals stored R_1 or not. If not, user is not the genuine owner of smart card. If true, reader generates a random nonce N_U, computes $LA_1 = h(h(SID_j||R_1 \oplus R_2)\ ||N_U)$ and sends the login request $\{ID_i, SID_j, N_U, LA_1\}$ to S_j.

U_i S_j

Login and Authentication Phase

Input the credentials ID_i and PW_i'
Compute $R_1 = h(ID_i||h(PW_i))$
Verify whether $R_1 = R_1$ or not
If true, generate a random nonce N_U
Compute $LA_1 = h(h(SID_j||R_1 \oplus R_2)\ ||N_U)$

$\{ID_i, SID_j, N_U, LA_1\}$ →

Check the validity of ID_i
If true, compute $LA_1 = h(R_3||N_U)$
Verify whether computed LA_1 = received LA_1 or not
If true, generate a random nonce N_S,
Compute $SKey_{ij} = h(ID_i||\ SID_j||R_3||N_U||N_S)$
$LA_2 = h(SKey_{ij}||N_S)$

← $\{ID_i, LA_2, N_S\}$

Compute $SKey_{ij} = h(ID_i||SID_j||h(SID_j||R_1 \oplus R_2)||N_U||N_S)$
$LA_2 = h(SKey_{ij}||N_S)$
Verify whether computed LA_2 = received LA_2 or not
If it holds, compute $LA_3 = h(SKey_{ij}||N_U||N_S)$

$\{ID_i, LA_3\}$ →

Compute $LA_3 = h(SKey_{ij}||N_U||N_S)$
Verify whether computed LA_3 = received LA_3 or not

Figure 2. Proposed login and authentication phases

Authentication Phase :

Upon receiving the login request $\{ID_i, SID_j, N_U, LA_1\}$; S_j first checks the validity of ID_i to accept/reject the login request. If true, S_j computes $LA_1 = h(R_3||N_U)$ and then checks whether computed LA_1 equals received LA_1 or not. If it holds, S_j generates a nonce N_2, computes the session key $SKey_{ij}$, where $SKey_{ij} = h(ID_i||\ SID_j||R_3||N_U||N_S)$, $LA_2 = h(SKey_{ij}||N_S)$ and sends the message $\{ID_i, LA_2, N_S\}$ to U_i.

After getting the message $\{ID_i, LA_2, N_S\}$ from S_j, U_i computes $SKey_{ij} = h(ID_i||SID_j||h(SID_j||R_1 \oplus R_2)||N_U||N_S)$ and $LA_2 = h(SKey_{ij}||N_S)$ and checks whether the computed LA_2 equals received LA_2 or not. If it holds, S_j is authentic otherwise terminate the session. Subsequently, U_i computes $LA_3 = h(SKey_{ij}||N_U||N_S)$ and sends $\{ID_i, LA_3\}$ to S_j. Once the message $\{ID_i, LA_3\}$ is received, S_j computes $LA_3 = h(SKey_{ij}||N_U||N_S)$ and checks whether computed LA_3equals received LA_3 or not. If it holds, mutual authentication is achieved. Both the

parties agree upon a common shared session key $SKey_{ij} = h(ID_i||SID_j||h(SID_j||R_1 \oplus R_2)||N_U||N_S) = h(ID_i||SID_j||R_3||N_U||N_S)$

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 $R_1 = h(ID_i||h(PW_i))$ and verifies whether computed R_1 equals stored R_1 or not. If true, U_i enters a new password PW_{inew}. The smart card computes $R_{1new} = h(ID_i||h(PW_{inew}))$, $R_{2new} = R_{1new} \oplus R_2 \oplus R_1$ and stores R_{1new}, R_{2new} instead of R_1, R_2 respectively in the smart card memory. Thus, U_i can update the password without taking any assistance from S_j.

III. 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.

User Impersonation Attack :

In this proposed scheme, the login request contains $\{ID_i, SID_j, N_U, LA_1\}$. It contains $LA_1 = h(h(SID_j||R_1 \oplus R_2)||N_U)$. In order to securely perform impersonation attack, the attacker needs to guess the correct values of $h(PW_i)$ and $h(x)$.

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 $\{ID_i, LA_2, N_S\}$ is prepared by using the secret parameter (R_3) which can be computed by S_j only. Hence, the proposed authentication scheme prevents server spoofing.

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_u and N_s. So attackers cannot enter the system by resending the earlier transmitted messages to pretend to be legal users.

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., $\{ID_i, SID_j, N_U, LA_1\}$, $\{ID_i, LA_2, N_S\}$ and $\{ID_i, LA_3\}$. There

is no symmetry in the values of $LA_1 = h(h(SID_j||R_1 \oplus R_2)||N_U)$, $LA_2 = h(SKey_{ij}||N_S)$ and $LA_3 = h(SKey_{ij}||N_U||N_S)$. 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.

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.

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.

Security of the Session Key :

In this proposed multi-server authentication scheme, the session key $SKey_{ij} = h(ID_i||SID_j||h(SID_j||R_1 \oplus R_2)||N_U||N_S) = h(ID_i||SID_j||R_3||N_U||N_S)$ is associated with $h(x)$ which is 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.

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.

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.

Single Registration :

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

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' 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.

User can choose and update the password securely without taking any support from the server or registration center :

In the scheme, valid users 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.

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 $R_1 = h(ID_i||h(PW_i'))$ with the stored y_i during the login phase. Hence, the scheme provides early wrong password detection.

Each server uses unique secret parameter :

In the scheme, each server has unique secret parameter $R_3 = h(SID_j||h(x))$ used to authenticate the user. Hence, there is no need to store the secret parameter of all the servers in the smart card memory.

The scheme achieves mutual authentication and session key agreement :

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 $SKey_{ij} = h(ID_i||SID_j||h(SID_j||R_1 \oplus R_2)||N_U||N_S) = h(ID_i||SID_j||R_3||N_U||N_S)$ will be different for each login session.

The scheme solves time synchronization problem :

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

IV. PERFORMANCE COMPARISON

This section describes comparison among various multi-server authentication schemes with our 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. 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 our Proposed Scheme

Security Features	Juang [18]	Liao-Wang [21]	Hsiang-Shih [23]	Sood et al. [24]	Tyagi et al. [25]	Proposed Scheme
F1	No	Yes	Yes	No	Yes	**Yes**
F2	Yes	Yes	Yes	Yes	Yes	**Yes**
F3	No	Yes	Yes	Yes	Yes	**Yes**
F4	Yes	Yes	Yes	Yes	Yes	**Yes**
F5	Yes	Yes	Yes	Yes	Yes	**Yes**
F6	No	Yes	Yes	Yes	Yes	**Yes**
F7	Yes	Yes	No	No	Yes	**Yes**
F8	Yes	Yes	Yes	Yes	Yes	**Yes**
F9	Yes	No	No	Yes	Yes	**Yes**
F10	Yes	No	No	Yes	**No**	**Yes**
F11	Yes	Yes	No	Yes	Yes	**Yes**
F12	Yes	Yes	No	Yes	Yes	**Yes**
F13	Yes	Yes	Yes	Yes	Yes	**Yes**
F14	Yes	Yes	Yes	Yes	Yes	**Yes**
F15	Yes	Yes	Yes	Yes	Yes	**Yes**

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

H = One Way Hash Function
En = Symmetric Encryption
De = Symmetric Decryption
Ex = Modular Exponentiation

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

Authentication Schemes	Registration Phase	Login and Authentication Phase	Total
Juang [18]	3H + 1En	5H + 3En + 4De	8H + 4En + 4De
Liao-Wang [21]	5H	16H	21H
Hsiang-Shih [23]	7H	23H	30H
Sood et al. [24]	5H	25H	30H
Tyagi et al. [25]	5H + 2Ex	7H + 16Ex	12H + 18Ex
Proposed Scheme	**3H**	**11H**	**14H**

V. CONCLUSION

It is clear from these tables 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 comprise:

- It doesn't need verification table. It needs only secret key and doesn't need any secret number.
- 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 keeps away from the time-synchronization problem.

REFERENCES

[1] Needham, R. M. & Schroeder, M. D. (1978). Using encryption for authentication in large networks of computers. Communications of the ACM, 21(12), 993-999.

[2] Booth, K. S. (1981). Authentication of signatures using public key encryption. Communications of the ACM, 24(11), 772-774.

[3] Lamport, L. (1981). Password authentication with insecure communication. Communications of the ACM, 24(11), 770-772.

[4] Chang, C. C. & Wu, T. C. (1991). Remote password authentication with smart cards. IEE Proceedings on Computers and Digital Techniques, 138(3), 165-168.

[5] Hwang, M. S. & Li, L. H. (2000). A new remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, 46(1), 28-30.

[6] Sun, H. M. (2000). An efficient remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, 46(4), 958-961.

[7] Chien, H. Y., Jan, J. K. & Tseng, Y. M. (2002). An efficient and practical solution to remote authentication: smart card. Computers and Security, 21(4), 372-375.

[8] Hwang, M. S., Lee, C. C. & Tang, Y. L. (2002). A simple remote user authentication scheme. Mathematical and Computer Modeling, 36(1-2), 103-107.

[9] Ku, W. C. & Chen, S. M. (2004). Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, 50(1), 204-207.

[10] Yoon, E. J., Ryu, E. K. & Yoo, K. Y. (2004). Further improvement of an efficient password based remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, 50(2), 612-614.

[11] Yoon, E. J., Ryu, E. K. & Yoo, K. Y. (2005). An improvement of Hwang-Lee-Tang's simple remote user authentication scheme. Computers and Security, 24(1), 50-56.

[12] Wang, X. M., Zhang, W. F., Zhang, J. S. & Khan, M. K. (2007). Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards. Computer Standards and Interfaces, 29(5), 507-512.

[13] Das, M. L., Saxena, A. & Gulati, V. P. (2004). A dynamic ID-based remote user authentication scheme. IEEE Transactions on Consumer Electronics, 50(2), 629-631.

[14] Liao, I. E., Lee, C. C. & Hwang, M. S. (2005). Security enhancement for a dynamic ID-based remote user authentication scheme. In Proceedings of the NWeSP, pp. 437-440, Seoul, Korea, 2005.

[15] Wang, Y. Y., Liu, J. Y. Xiao, F. X. & Dan, J. (2009). A more efficient and secure dynamic ID-based remote user authentication scheme. Computer Communications, 32(4), 583-585.

[16] Hao, Z. & Yu, N. (2010). A security enhanced remote password authentication scheme using smart card. In Proceedings of the 2nd ISDPE, pp. 56-60, Buffalo, New York, USA, 2010.

[17] Song, R. (2010). Advanced smart card based password authentication protocol. Computer Standards and Interfaces, 32(5-6), 321-325.

[18] Juang, W. S. (2004). Efficient multi-server password authenticated key agreement using smart cards. IEEE Transactions on Consumer Electronics, 50(1), 251-255.

[19] Ku, W. C. & Chuang, H. M. (2005). Weaknesses of a multi-server password authenticated key agreement scheme. National Computer Symposium, 1-5.

[20] Chang, C. C. & Lee, J .S. (2004). An efficient and secure multi-server password authentication scheme using smart cards. Proceedings of International Conference on Cyberworlds, 417-422.

[21] Liao, Y. P. & Wang, S. S. (2009). A secure dynamic ID based remote user authentication scheme for multi-server environment. Computer Standards & Interfaces, 31(1), 24-29.

[22] Chen, T. Y., Hwang, M. S., Lee, C. C. & Jan, J. K. (2009). Cryptanalysis of a secure dynamic ID based remote user authentication scheme for multi-server environment. Fourth International Conference on Innovative Computing, Information and Control, 725-728.

[23] Hsiang, C. & Shih, W. K. (2009). Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment. Computer Standards & Interfaces, 31(6), 1118-1123.

[24] Sood, S. K., Sarje, A. K. & Singh, K. (2011). A secure dynamic identity based authentication protocol for multi-server architecture. Journal of Network and Computer Applications, 34(2), 609-618.

[25] Tyagi, J. K., Srivastava, A. K. & Patwal P. S. (2012). Remote user authentication scheme in multi-server environment using smart card. International Journal of Computer Applications, 57(12) 1-5.