An Enhanced Secure Remote User Authentication Scheme without Verification Table

Sumitra Binu
Research scholar
Christ University
Bangalore, India

Pethuru Raj, Ph.D
Cloud Solution Architect
IBM Global Cloud Center of Excellence,
IBM India, Bangalore

M. Misbahuddin, Ph.D
Senior Technical Officer
C-DAC, Electronic City
Bangalore, India

ABSTRACT
With the significant advances in communication networks over the last few decades, smart cards have been widely used in many e-commerce applications and network security protocols due to their low cost, portability, efficiency and cryptographic properties. In this paper, we analyze Sood et al.'s smart card based authentication scheme and demonstrate that the scheme is vulnerable to masquerade user attack, offline password guessing attack, time concurrency weaknesses and fails to achieve mutual authentication. A secure dynamic identity based remote user authentication scheme without verification tables, is proposed in this paper and the scheme resolves the aforementioned problems of Sood et al.'s scheme. The computation cost of the proposed scheme is comparable to Sood et al.'s scheme and it is highly secure taking into consideration the complexity of calculating discrete logarithms and the resistance to various attacks.

General Terms
Security

Keywords
Remote User Authentication, Smart Cards, No Verification Table, Cyclic groups, Discrete Logarithm

1. INTRODUCTION
Password based authentication protocols is the most commonly used mechanism carrying out remote user authentication. Many research works depicting the application of password-based authentication schemes with smart cards to verify the legitimacy of remote user login requests have already been published [1, 2, 3, 4, 5, 6, 7]. In 1981, Lamport [8] proposed a password based authentication scheme though it failed to preserve user anonymity. In 2004, Das et al., [9] proposed a user anonymity preserving, dynamic identity based remote user authentication scheme. Later the scheme was proved to be susceptible to insider attack, masquerade attack and server spoofing attack [10, 11, 12]. Chien and Chen [13] proposed an improvement of Das et al.'s scheme, but is highly computation intensive. In 2005, Liao et al., [14] proposed a scheme that enhances the security of Das et al.'s scheme and supports mutual authentication but Yoon and Yoo [15] demonstrated a reflection attack on their scheme. In 2006, Liou et al., [16] suggested a new dynamic identity based remote user mutual authentication scheme and Shih [17] demonstrated that their scheme fails to achieve mutual authentication. Hsiang and Shih in 2009[18] proposed a remote user authentication scheme. This scheme was found to be susceptible to server spoofing attack, replay attack and password guessing attackby Sood et al. [19]. Again in 2010, Sood et al. [19] proved that Liou et al.'s scheme is susceptible to Ku et al.'s impersonation attack [20] and proposed a modified scheme. Kwang Cheul Shin and Jung Gil Cho[21] pointed out that Sood et al.'s scheme is vulnerable to steal information from database attack , insider attack etc. In this paper, it is demonstrated that Sood et al.'s scheme is also susceptible to masquerade user attack, database attack etc. and propose a modified version which resolves the weaknesses of Sood et al.'s scheme. The discussed scheme preserves user anonymity and does not require the server to maintain a verification table which in turn resists the stolen verifier attack

The rest of the paper is organized as follows. In section 2, a brief overview of Sood et al.'s scheme [19] is given. Section 3 describes the weaknesses of Sood et al.'s scheme. Section 4, discusses the proposed scheme and security analysis of the scheme is presented in Section 5. Cost and functionality comparison is shown in section 6 and section 7 concludes the work done.

2. REVIEW OF SOOD ET AL.'S SCHEME
This section includes a brief overview of Sood et al.'s scheme. The scheme involves two participants' viz., the user U and the Server S. There are four phases in this scheme which includes the Registration, login, authentication and password change phase. During the registration phase a user submits his identity, ID and password, PW to S. S computes the security parameter's using his secret key x and random value y, stores the same in a smart card (SC) and sends it to the user U via a secure channel. During the login phase, U inserts the SC and types in his ID and PW. The SC verifies the authenticity of the user by checking the password and then creates the login request. The request is sent by U to S. During the authentication phase, U and S mutually authenticate each other and the password change phase allows the user to change the password without the intervention of S. To shorten the length of the paper, we omit the review. Please refer to [19] for Sood et al.'s protocol.

3. WEAKNESSES OF SOOD ET AL.'S SCHEME
Kwang Cheul Shin and Jung Gil Cho[21] pointed out that Sood et al.'s scheme is vulnerable to stolen verifier attack , insider attack etc. This section demonstrates that the protocol is also susceptible to impersonation attack, time concurrency weaknesses and fails to preserve user anonymity.

3.1 Offline Secret Key Guessing Attack
A valid but malicious user can extract the security parameters B_i, C_i and D_i stored in the memory of his smart card and can extract h(x) from D_i using his own ID_i and P_i. Then the adversary can try to guess different values of x and check its correctness by verifying it with the value of h(x).

3.2 Time Concurrency Weakness

Sood et al.'s scheme uses time concurrency mechanism to resist replay attacks possible during an authentication session. Studies shows that the usage of time stamps are susceptible to certain drawbacks such as different time zones of Client and Server, delivery latency etc. [7]. The lack of synchronization of clocks of the participants can lead to the failure of the authentication scheme.

3.3 Denial of Service Attack

An adversary U_k, who gets hold of the smart card(SC) of a registered user U_i can extract the parameters B_i, C_i and D_i using various side-channel attacks. Then U_k modifies B_i to B_i*. When U_i tries to login later by using his SC and entering ID_i and P_i , the SC computes $h(x\| y_i)^* = B_i^* \oplus h(ID_i\| P_i) \oplus P_i$. Then SC calculates $C_i^* = h(x\| y_i)^* \oplus h(P_i)$ and compares C_i^* with C_i. There will be a mismatch since B_i was modified and hence U_i will be denied service. DOS to a valid user also happens when an administrator updates any secret information specific to a valid user, which is stored in the database of the server. In Sood et al.'s scheme, the server maintains a data base that stores the secret information of valid users. If a malicious administrator modifies this information, then a registered user will not be able to login to the server with his valid credentials.

3.4 Masquerade Server Attack

If a malicious user U_i attempts to impersonate the server S, she must be able to forge a valid challenge (V_i , T "). U_i can get h(x) from his own smart card. Then if he intercepts a legitimate user U_k's login request, he can obtain (CID_k, M_k , T). He calculates, $h(x\| y_k) = CID_k \oplus h(h(x) \|T)$. Again, if U_i intercepts the server's response (V_i , T"), he can generate his own version of the response as (V_{im} , T") where $V_{im} = ((h(x\| y_k) \| h(x) \|T \|T")$ and send (V_{im}, T") to the user U_k .

3.5 Impersonation Attack

In this attack a malicious user U_i tries to forge a valid login request message (CID_V , M_V ,T) sent by the valid user where CID_V , M_V are the CID and M values , of a valid registered user. Let us assume the following attack scenario.

The malicious valid User U_i has his own smart card from which he extracts B_i , C_i and D_i. Computes $h(x) = D_i \oplus h(ID_i\| P_i)$ using his own ID_i and P_i. h(x) is common for all valid users. At the login phase, the valid user U_v sends (CID_V , M_V , T) to S. Then U_i can eavesdrop on the login request of the valid user U_V. U_i computes $h(x\| y_V) = CID_V \oplus h(h(x) \|T)$, CID ' = $h(x\| y_V) \oplus h(h(x) \|T')$ where T ' is the current date and time of U_i. U_i computes M' = (h(h(x) ||h(x|| y_V) || T'). Here CID' and M' are U_i's version of CID_V and M_V respectively. U_i sends (CID', M', T') to the server. In this case, T ' is valid since it is computed by U_i with the current date and time. Upon receiving the login request, S verifies the validity of T '. If true, S accepts the request and computes $A_i^* = h(x\| y_i)^* = h(x\| y_V) = CID' \oplus h(h(x) \| T')$. S retrieves $y_V \oplus x$ and $ID_V \oplus h(x)$ corresponding to $A_i = A_i^*$ from its database. S extracts y_V from $y_V \oplus x$ and ID_V from $ID_V \oplus h(x)$, since it knows x. S computes $M_V^* = h(h(x) \|A_i \| T')$ and compare M_V^* with M' in the received login request. Here the condition will surely hold and S will accept the login request. S computes $V_i = h(A_i \| h(x) \| T_s \| T')$, where T_s is the server's current date and time. S sends (V_i , T_s) to the smart card of valid user and U_i intercepts the same. The malicious valid user U_i impersonates his peer valid user U_L and he can carry forward the communication if he can find the ID of U_L, and generate the session key.

3.6 Offline Password Guessing Attack

In case a malicious valid user U_i , gets the smart card of another registered user U_k , then he will be able to extract its contents. Then if U_i intercepts a previous login request, (CID_k, M_k,T) of U_k, he can extract $h(x\| y_k)$ from CID_k as $h(x\| y_k) = CID_k \oplus h(h(x) \|T)$ since he knows h(x) and T. Now U_i can calculate $h(P_k) = C_k \oplus h(x\| y_k)$ since he has extracted C_k from the smart card and $h(x\| y_k)$ from the login request message respectively of user U_k. He can guess the value of P_k to be P_k * from a dictionary space D_{pw}. Computes $h(P_k$ *) and compares it with $h(P_k)$. The process is repeated until a match is found.

4. PROPOSED SCHEME

The vulnerabilities of Sood et al.'s scheme is mainly due to the fact that the valid user can easily calculate the values of $h(x\| y_i)$ and h(x) as computed by the server S and this should be prevented. Also the verification table makes the scheme vulnerable to stealing information from database attack and ID-theft attack. Taking into consideration the above mentioned vulnerabilities a remote user authentication scheme that eliminates the requirement of verification table is proposed. The scheme which attempts to address the flaws of Sood et al.'s scheme consists of four phases' viz., Initialization, Registration, Login & and Password change phase as summarized in figure 1. The notations used are listed in Table1.

Table 1. Notations

U_i, S	i th User , Server
ID_i, P_i	Unique Identification of U_i, Password of user U_i
Z_n	Additive Cyclic group, integer modulo 'n
g0	Generator of cyclic group
a, b_i	Server's secret key, Random number selected by S unique to each U_i
r	Random number generated by smart card , unique to each session
h(.) , ⊕ , ||	One way hash function, XOR operation, Concatenation Operation
⇒	Secure Communication Channel

4.1 Initialization Phase

Given a finite additive cyclic group $Z_n = < g_0>$, of order q where q is a prime number. Element g_0 is a generator of Z_n and is kept as a secret between the user and the server.

4.2 Registration Phase

A user U_i who wants to become a registered member of the system chooses her identity ID_i and password P_i. U_i computes $x = h(P_i)$, $y = g_0^x$, $h(ID_i)$ and submits ($h(ID_i)$, y) to server through a secure communication channel. Server S chooses the value 'a' as its secret key and a random number 'b_i' where a, $b_i \in Z_n$ and computes the following: $A_i = h(a||b_i)$; $B_i = h(h(ID_i) ||y) \oplus y \oplus h(a||b_i)$; $C_i = h(a||b_i) \oplus y$; $D_i = h(h(ID_i) ||y) \oplus h(a)$. S ⇒ SC : ($B_i$, C_i, D_i and h(.)) . U_i stores g_0 in the smart card which now contains, (B_i, C_i, D_i, g_0 and h(.))

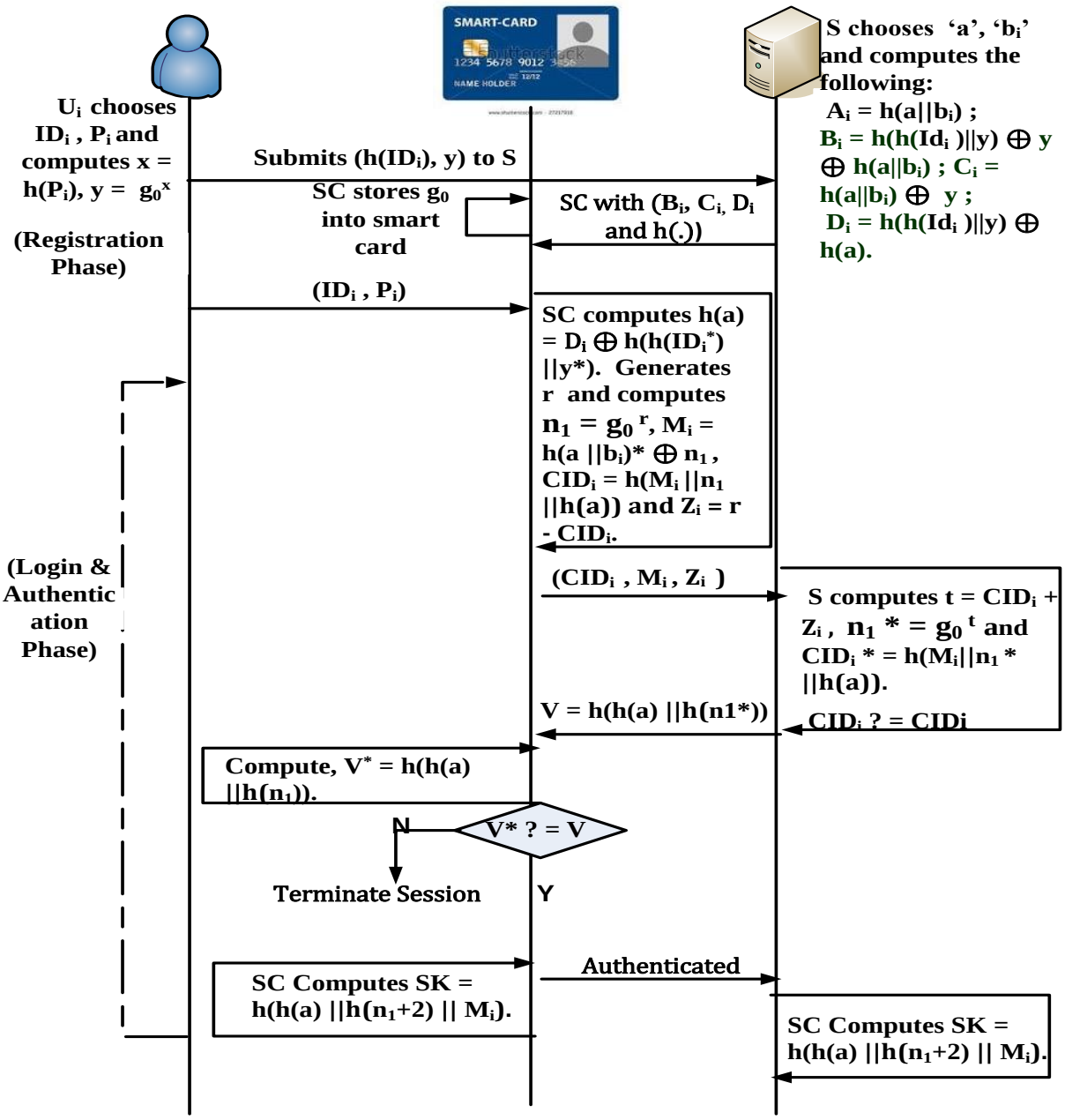

Fig 1: Phases of Proposed Protocol

4.3 Login and Authentication Phase

Whenever a registered user U_i wants to login, he inserts his SC into the reader and inputs ID_i^* and P_i^*. Then SC computes $x^* = h(P_i^*)$ and $y^* = g_0^{x^*}$, $A_i^* = h(a||b_i)^* = C_i \oplus y^*$, $B_i^* = h(h(ID_i^*)||y^*) \oplus y^* \oplus h(a||b_i)^*$. SC checks $B_i^* = B_i$. If the equality does not hold, SC rejects the request. Otherwise, the identity of the U_i is validated and the SC computes the login request as follows and sends it to the server. SC computes $h(a) = D_i \oplus h(h(ID_i^*)||y^*)$. SC generates a random number $r \in Z_n$ and computes $n_1 = g_0^r$, $M_i = h(h(a||b_i)^* || r \oplus n_1)$, $CID_i = h(M_i||n_1||h(a))$ and $Z_i = r - CID_i$. Then SC $\Rightarrow$ S: (CID_i , M_i , Z_i). In this phase, there is a limit on the number of attempts a user can make to login to the server after which, the smart card gets locked.

4.4 Password Change Phase

A registered user can change the password at his will, without the intervention of the server. U_i inputs ID_i^* and P_i^* . SC computes $x^* = h(P_i^*)$, $y^* = g_0^{x^*}$, $h(a||b_i)^* = C_i \oplus y^*$, $B_i^* = h(h(ID_i^*)||y^*) \oplus y^* \oplus h(a||b_i)^*$. SC compares $B_i^* = B_i$. If the equality does not hold, SC rejects the request. If the verification holds, the identity U_i is validated and SC prompts the user to enter the new password P_i^{new}. Then SC computes $x_{new} = h(P_i^{new})$, $y_{new} = g_0^{X_{new}}$, $h(a)^* = D_i \oplus h(h(ID_i^*)||y)$. SC computes $B_i^{new} = h(h(ID_i^*)||y_{new}) \oplus y_{new} \oplus h(a||b_i)^*$, $C_i^{new} = h(a||b_i)^* \oplus y_{new}$, $D_i^{new} = h(h(ID_i^*)||y_{new}) \oplus h(a)^*$. SC updates the values of B_i, C_i and D_i stored in the memory of the smart card with the values B_i^{new} , C_i^{new} , D_i^{new}.

5. SECURITY ANALYSIS

This section examines the resistance of the proposed scheme to various possible attacks on remote user authentication scheme.

5.1 Impersonation Attack

This attack attempts to forge the message by using the information obtained from the target authentication scheme.

When forging the message, the attacker disguises as a legal user. The attacker attempts to modify the message (CID_i , M_i , Z_i). But the attacker needs to know the secret key 'a' of the server, random number 'b_i' chosen by server uniquely for user U_i and the client's random number 'r'and nonce 'n_1' , to compute the valid values of CID_i , M_i , Z_i . Otherwise the attempts would be rejected at the authentication phase. Additionally the disguise attack is impossible because' r'is a session variable which is valid only for a single session and the session ID's are well protected to prevent a session hijacking attack. Moreover, the attacker should know 'n_1' to calculate the session key to carry forward the communication. Hence the proposed scheme is secure against, forgery or impersonation attack.

5.2 Insider Attack

In the registration phase, the user submits $y = g_0^x$, where x = h(password) to the server. So, even an insider cannot know the password of a user, since computing x from y involves the solving the discrete logarithm problem. Here g_0 is a generator of the additive cyclic group Z_n, where Z_n is group of integer's modular 'n'. Calculating the discrete logarithm of values generated using modular arithmetic is a computationally intensive task which makes the scheme secure against insider attack.

5.3 Stolen Verifier Attack

The proposed scheme does not require the server to maintain a verification table. Hence **t**his attack which involves copying the authentication parameters stored in a verifier table and using the same to impersonate a valid user does not have any relevance here.

5.4 Time Concurrency Weaknesses

Sood et al.'s scheme uses time stamps to avoid replay attacks. Time stamps require proper synchronization of clocks at the ends of both the serer and the client and this may have practical difficulties when the client and server belong to different time zones.. The proposed scheme overcomes this limitation by using nonce values.

5.5 Security against Denial of Service Attack

The proposed scheme prevents unauthorized modification of password verification information by enabling the smart card to check the validity of user before updating the password. It is impossible to correctly guess ID_i and P_i both simultaneously even after getting the SC of the legitimate user. Also an administrator cannot modify the password information in database, since there is no verification table maintained by the server.

5.6 Offline Password Guessing Attack

In this attack an attacker first tries to obtain some client or server verification information containing the password parameter and tries to guess the password offline. In the proposed scheme the password 'P_i ' is neither transmitted nor stored in the smart card in its bare form. The password is stored and transmitted as $y = g_0^x$, where $x = h(P_i)$. To get the password 'x' the attacker should calculate the discrete logarithm of 'y' to the base g_0 and calculation of discrete logarithms in modular arithmetic is a computationally intensive and time consuming process. Thus the complexity involved in solving discrete logarithmic problem, makes the proposed scheme secure against offline password guessing attack.

5.7 Attack on User Anonymity

In Sood et al.'s scheme, the attacker is able to easily extract $h(x\| y_i)$, from the login request message. This value which is unique to a particular user, will be the same in all login request messages providing the attacker to trace the messages as belonging to a particular user. In the proposed scheme, even though the unique value $h(a||b_i)$ is used in the login request message , it cannot be extracted by the attacker. This prevents him from tracing out the valid user and preserves user's anonymity.

6. COST AND FUNCTIONALITY ANALYSIS

The comparison of the proposed scheme with Sood et al.'s scheme is summarized in Table 2 and 3 respectively. This scheme assumes that the parameters ID_i, P_i, a, b_i, r are 128-bit long. We use SHA-2 a more secure hash function whose output is 256 bits long.

Table 2. Functionality Comparison

	Proposed Scheme	**Sood et al.[19]**	**Liao-Wang[11]**	**Hsiang-Shih[18]**
Resists Impersonation Attack	Yes	No	No	No
Resists Password Guessing Attack	Yes	No	Yes	No
Overcomes Time Concurrency Weaknesses	Yes	No	Yes	Yes
Resists Denial-of-Service Attack	Yes	No	Yes	Yes
Resists Stolen Verifier Attack	Yes	No	Yes	No
Insider Attack	Yes	No	No	Yes
Provides Mutual Authentication	Yes	Yes	yes	yes
Provides Session Key Agreement	Yes	Yes	yes	Yes

Let T_H and T_E denote the time complexity for hashing, exponentiation and symmetric key encryption respectively. In the proposed scheme, the parameters stored in the smart card are B_i, C_i , D_i and g_0 and hence E1, the memory needed in the smart card is 896 bits. Communication cost of authentication (E2) includes the capacity of transmitting message involved in the authentication. The capacity of transmitting message (CID_i , M_i , Z_i) and V_i is 1024 bits. The computation cost of registration (E3) is the total time of all operations executed in this phase. The computation cost of the user (E4) and the service provider (E5) is the time spent by the user and

the service provider during the process of login, authentication and session key agreement.

Table 3. Cost Comparison of Proposed Scheme and Sood et al.'s Scheme

	Proposed Scheme	**Sood et al.[19]**
E1	896(= 3* 256 + 128) bits	384 bits
E2	1024(= 4 *256) bits	640 bits
E3	$T_E + 6T_H$	$4T_H$
E4	$2T_E + 5T_H$	$6T_H$
E5	$T_E + 3T_H$	$5T_H$

7. CONCLUSION

In 2006, Liou et al. proposed a password authentication scheme using smart cards ,to overcome the security limitations of the dynamic ID based authentication scheme proposed by Das et al. However, in 2010, Sood et. al., demonstrated that Liou at al.' scheme is not resistant to malicious user attack, man in the middle attack, impersonation attack and offline password guessing attack and they proposed a modification. This paper analyzes the weaknesses of Sood at al.'s scheme and proposes a modified version without verification table. The proposed scheme enhances security by using cyclic groups as the domain for generating the security parameters and by exploiting the difficulty in solving discrete logarithmic problem in modular arithmetic. Future scope of this work is to increase efficiency by reducing the computation cost and enhance security by making the protocol resistant to more attacks.

8. REFERENCES

[1] W.C. Ku, S.M. Chen, "Weakness and Improvement of an Efficient Password Based Remote User Authentication Scheme Using Smart Cards," IEEE Transactions on Consumer Electronics 50(1), 204-207 (2004)

[2] Y.C. Chen, L.Y. Yeh, " An Efficient Nonce-Based Authentication Scheme with Key Agreement," Applied Mathematics and Computation 169(2), 982-994 (2005)

[3] W.G. Shieh, J.M. Wang, "Efficient Remote Mutual Authentication and Key Agreement," Computers and Security 25(1), 72-77 (2006)

[4] H.C Hsiang, W.K. Shih,"Weakness and Improvement of Yoon-Ryu-Yoo Remote User Authentication Scheme Using Smart Cards," Computer Communications 32(4), 649-652 (2009)

[5] M.Kumar, "A New Secure Remote User Authentication Scheme with Smart Cards", International Journal of Network Security 11, 88-93 (2010)

[6] S.K. Sood, A.K Sarje, K.Singh, "A Secure Dynamic Identity-Based Remote User Authentication Scheme," In:T. Janowski, H. Mohanty. (eds) ICDCIT 2010. LNCS, vol. 5966, pp.224-235, Springer, Heidelberg (2010)]

[7] M.Misbahuddin, A.A. Mohammed, M.H. Shastri, "A Simple and Efficient Solution to Remote User Authentication using Smart Cards," In Proceeding of International Conference on Innovations in Information Technology (IIT '06), Dubai,Nov.2006, pp.1-5.

[8] L. Lamport, "Password Authentication with Insecure Communication," Communications of the ACM, vol. 24. no. 11, pp. 770-772, November 1981

[9] M.L. Das, A. Saxena and V.P. Gulati," A Dynamic ID-Based Remote User Authentication Scheme, " IEEE Transactions on Consumer Electronics, vol. 50, no.2, pp. 629-631, May 2004

[10] T. Goriparthi, M.L. Das, A.Saxena, "An Improved Bilinear Pairing Based Remote User Authentication Scheme," Computer Standards and Interfaces 2009, 31 : (181-185)

[11] Y.P. Liao, S.S. Wang, "A Secure Dynamic ID Based Remote User Authentication Scheme for Multi Server Environment," Computer Standards and Interfaces 2009, 31(1): 24-29

[12] Y.Y. Wang, J.Y. Liu, F.X. Xiao, J.Dan, "A More Efficient and Secure Dynamic ID Based Remote User Authentication Scheme," Computer Communications, 2009, 32(2): 583-585

[13] H.Y Chien and C.H. Chen, "A Remote Authentication Scheme Preserving User Anonymity," In Proceedings of Advanced Information Networking and Applications, vol.2, pp. 245-248, March 2005

[14] I.E. Liao, C.C.Lee and M.S. Hwang, "Security Enhancement for a Dynamic ID-Based Remote User Authentication Scheme," In Proceeding of Conference on Next Generation on Web Services Practice, pp. 437-440, July 2005

[15] [15] E.J. Yoon and K.Y. Yoo, " Improving the Dynamic ID-Based Remote Mutual Authentication Scheme," In Proceedings of OTM Workshops 2006, LNCS 4277, pp. 499-507, July 2006

[16] Y.P Liou, J.Lin and S.S. Wang, " A New Dynamic ID-Based Remote User Authentication Scheme Using Smart Cards," In Proceedings of 16th Information Security Conference, Taiwan, pp. 198-205, July 2006

[17] H.C. Shih, "Cryptanalysis on Two Password Authentication Schemes," Laboratory of Cryptography and Information Security, National Central University, Taiwan, July 2008

[18] H.C. Hsiang and W.K. Shih, "Improvement of the Secure Dynamic ID Based Remote User Authentication Scheme for Multi-Server Environment", Computer Standards & Interfaces, vol.31, **(2009)**, pp.1118-1123

[19] S.K. Sood. A.K. Sarje and K.Singh, "An Improvement of Liou et al.'s Authentication Scheme Using Smart Cards," International Journal of Computer Applications, vol.1, no.8, (2010), pp.16-23

[20] W.C. Ku and S.T. Chang, "Impersonation Attack on Dynamic ID-Based Remote User Authentication Scheme using Smart Cards," IEICE Transactions on Communications, vol. E88-B, No.5, pp.2165-2167, May 2005

[21] C.S. Kwang and G.C. Jung, "An Improvement of Sood et al.'s Authentication Scheme using Smart Card", International Journal of Security and Its Applications, vol. 7, No. 3, May, 2013