Rev. Fac. Ing. Univ. Antioquia N.° 68 pp. 27-35. Septiembre, 2013

Cryptanalysis and improvement of Chen-Hsiang-Shih's remote user authentication scheme using smart cards

Criptoanálisis y mejora del esquema de autenticación de usuarios remotos utilizando tarjetas inteligentes propuesto por Chen-Hsiang-Shish

Rafael Martínez-Peláez[*1], *Francisco Rico-Novella*[2], *Pablo Velarde-Alvarado*[3]

[1]Instituto de Informática, Universidad de la Sierra Sur. Calle Guillermo Rojas Mijangos S/N. C.P. 70800. Miahuatlán de Porfirio Díaz, Oaxaca, México.

[2]Departamento de Ingeniería Telemática, Universidad Politécnica de Cataluña. Calle Jordi Girona 31. C.P. 08034. Barcelona, España.

[3]Área de Ciencias Básicas e Ingenierías, Universidad Autónoma de Nayarit, Ciudad de la cultura – Amado Nervo. C.P. 63155. Tepic, Nayarit, México.

(Recibido el 28 de agosto de 2012. Aceptado el 5 de agosto de 2013)

Abstract

Recently, Chen-Hsiang-Shih proposed a new dynamic ID-based remote user authentication scheme. The authors claimed that their scheme was more secure than previous works. However, this paper demonstrates that their scheme is still unsecured against different kinds of attacks. In order to enhance the security of the scheme proposed by Chen-Hsiang-Shih, a new scheme is proposed. The scheme achieves the following security goals: without verification table, each user chooses and changes the password freely, each user keeps the password secret, mutual authentication, the scheme establishes a session key after successful authentication, and the scheme maintains the user's anonymity. Security analysis and comparison demonstrate that the proposed scheme is more secure than Das-Saxena-Gulati's scheme, Wang et al.'s scheme and Chen-Hsiang-Shih.

---------- *Keywords:* Cryptanalysis, mutual authentication, network security, session key agreement, smart cards

* Autor de correspondencia: teléfono: + 52 + 951 + 5 72 41 00, fax: + 52 + 951 + 1 32 53 30, correo electrónico: rpelaez@unsis.edu.mx (R. Martínez)

Resumen

Recientemente, Chen-Hsiang-Shih propusieron un nuevo esquema de autenticación de usuario remoto basado en un identificador dinámico. Los autores afirman que su esquema es más seguro que los trabajos previos. Sin embargo, se demuestra que su esquema continúa siendo inseguro contra diferentes tipos de ataques. Con el fin de mejorar la seguridad del esquema propuesto por Chen-Hsiang-Shih, se propone un esquema que consigue los siguientes objetivos de seguridad: el esquema no requiere de una tabla de verificación, cada usuario elige y cambia su contraseña libremente, cada usuario mantiene su contraseña en secreto, el esquema requiere autenticación mutua, el esquema establece una clave de sesión después de una autenticación correcta, y el esquema mantiene el anonimato del usuario. El análisis de seguridad y la comparación demuestran que nuestro esquema es más seguro que el esquema propuesto por Das-Saxena-Gulati, Wang-Liu-Xiao-Dan, y Chen-Hsiang-Shih.

---------- *Palabras clave:* Criptoanálisis, autenticación mutua, seguridad en redes, acuerdo de clave de sesión, tarjetas inteligentes

Introduction

A remote user authentication scheme is used to authenticate the legitimacy of each user over an open network. These schemes not only verify the identity of each user but also prevent attacks (e.g. server spoofing attack). For that reasons, such schemes are the first line of defense against adversaries.

The first remote user authentication scheme for an open network was introduced in [1]. The scheme is based on a one-way hash function, such as MD5 [2] or SHA [3]. Unfortunately, the scheme introduced in [1] requires that the server stores a password list, making it vulnerable to threats of revealing passwords in the directory [4] or modifying the verification table [5]. Two different schemes have been proposed [6] and [7] to remedy the security vulnerability of [1], both schemes work without a verification table. Then, a remote user authentication scheme with smart cards and without verification table was introduced in [4]. Since 1991, several remote user authentication schemes using smart cards [5, 8-18] have been proposed to enhance security and reduce vulnerabilities. Later, a dynamic ID-based remote user authentication scheme was proposed in [19]. The concept of dynamic ID prevents that an attacker can know the user's identity. However, the scheme is susceptible to the following attacks: impersonation [20], insider, masquerade, and server spoofing [21]. Moreover, the scheme proposed in [19] is insecure, because it can work like an open channel and does not provide mutual authentication [22, 23]. Since the scheme introduced in [19], several dynamic ID-based remote user authentication schemes [21, 24-39] have been proposed with the attempt to reduce security vulnerabilitiRecently, a new dynamic ID-based remote user authentication scheme has been proposed [21] and the authors claimed that their scheme resolves the security flaws of [4]. However, the scheme is vulnerable to denial of service attack, impersonation attack, parallel session attack, password guessing attack, and masquerading attack [26, 34, 36, 38, 40, 41]. In order to increase the security and reduce vulnerabilities of the scheme introduced in [21] an enhanced version [28] was proposed. However, this paper demonstrates that the scheme introduced in [28] is still insecure and presents a new scheme to overcome all the security weaknesses found in [28].

Review of Chen-Hsiang-Shih's dynamic ID-based remote user authentication scheme

A brief review of the scheme proposed in [28] is presented. The notations used throughout this paper are as follows:

U: User

ID: Identity of *U*

PW: Password of *U*

S: Server

x, y: Permanent secret key of *S*

h(): One-way hash function

h_p(): One-way hash function which includes a secret code s

||: String concatenation operation

⊗: Exclusive-or operation

Registration phase

This phase is invoked when *U* desires to be registered by *S*. The process is as follows:

1. *U* selects a random number *b* and computes using the equation (1):

$$h(b \otimes PW) \quad (1)$$

2. *U* sends (*ID*, h($b \otimes PW$)) to *S* through a secure channel
3. *S* performs the equations (2), (3) and (4):

$$P = h(ID \otimes x) \quad (2)$$

$$R = P \otimes h(b \otimes PW) \quad (3)$$

$$V = h_p(h(b \otimes PW)) \quad (4)$$

4. *S* stores *V*, *R*, *h*(), and h_p() in *U*'s smart card
5. *S* sends the smart card to *U* through a secure channel
6. Finally, *U* enters *b* into his smart card

Login phase

This phase is invoked whenever *U* requests to login *S*. The process is as follows:

1. *U* inserts smart card into the smart card reader, and keys *ID* and *PW*
2. *U*'s smart card performs the equations (5) and (6):

$$P = R \otimes h(b \otimes PW) \quad (5)$$

$$h_p(h(b \otimes PW))^* ?= V \quad (6)$$

3. *U*'s smart card generates a random number *r*, and performs the equations (7) and (8):

$$C_1 = P \otimes h(\mathrm{r} \otimes b) \quad (7)$$

$$C_2 = h_p(h(r \otimes b) \parallel T_U) \quad (8)$$

where T_U denotes *U*'s current timestamp

4. *U*'s smart card sends the login request message (*ID*, C_1, C_2, T_U) to *S*

Verification phase

This phase is invoked when *S* receives *U*'s login request message. The process is as follows:

1. If $(T_S - T_U) > \Delta T$, where denotes the expected valid time interval for transmission delay, then *S* rejects the login request; in other case, *S* continues with the process
2. *S* performs the equations (2), (9) and (8):

$$P^* = h(ID \otimes x) \quad (2)$$

$$h(r \otimes b)^* = P^* \otimes C_1 \quad (9)$$

$$C_2^* = h_p(h(r \otimes b)^* \parallel T_U) \quad (8)$$

3. If C_2^* is equal to the received C_2, *S* accepts *U*'s login request and computes the equation (10):

$$C_3 = h_p(h(r \otimes b)^* \otimes T_S \parallel P) \quad (10)$$

where T_S denotes *S*'s current timestamp

4. S sends (T_S, C_3) to U

   Upon receiving the message (T_S, C_3), U carries the following operations:

5. U verifies either T_S is invalid or $T_S = T_U$
6. U computes the equation (10):

   $C_3^* = h_p(h(r \otimes b)^* \otimes T_S \| P)$ (10)

7. If C_3^* is equal to the received C_3, U successfully authenticates S

   In addition, U and S compute the session key using the equation (11):

$$h(r \otimes b) \quad (11)$$

Password change phase

This phase is invoked whenever U desires to change PW. The process is as follows:

1. U inserts smart card into the smart card reader, keys ID and PW, and requests to change password
2. U's smart card computes the equations (5) and (4):

$$P^* = R \otimes h(b \otimes PW) \quad (5)$$

$$V^* = h_p(h(b \otimes PW)) \quad (4)$$

3. U's smart card verifies V^* and stored V in smart card
4. If V^* and V are equal, U chooses new password PW_{new}
5. U's smart card compute $R_{new} = P^* \otimes h(b \otimes PW)$ and $V^* = h_p(h(b \otimes PW))$, and then replaces R, V with R_{new}, V_{new}, respectively.

Cryptanalysis of Chen-Hsiang-Shih's dynamic ID-based remote user authentication scheme

A security analysis of the scheme proposed in [28] is presented. The security analysis demonstrates that the scheme is still vulnerable to an impersonation attack, server spoofing attack, and offline secret key guessing attack. In addition, the scheme fails to preserve U's anonymity.

Off-line secret key guessing attack

A legal but malicious user can know $P = h(ID \otimes x)$ from $R = P \otimes h(b \otimes PW)$ because it knows the correct PW. Then, the attacker can guess a candidate x^* to compute $P^* = h(ID \otimes x^*)$ until it finds P^* equals to P stored in the smart card. If $P^* = P$, means that, the intruder found the permanent secret key of S.

This attack is possible because S uses the same secret key for each user. Moreover, S uses the secret key in clear. It is obvious that the security of the entire system is compromised.

Impersonation attack

Suppose that a legal but malicious user intercepts a login request message (ID, C_1, C_2, T_U) of the victim and it knows x. Then, the intruder can perform an impersonation attack as follows:

1. Computes $P^* = h(ID \otimes x)$
2. Recovers $h(\mathrm{r} \otimes b)$ from C_1 computing $h(\mathrm{r} \otimes b) = P^* \otimes C_1$
3. Computes $C_1^* = P^* \otimes h(\mathrm{r} \otimes b)$ and $C_2^* = h_p(h(r \otimes b) \| T_{U*})$ where T_{U*} denotes attacker's current timestamp
4. Sends (ID, C_1^*, C_2^*, T_{U*}) to S

   Upon receiving the login request message from the attacker, S performs the following operations:

5. Since T_{U*} is valid, S computes $P^{**} = h(ID \otimes x)$, $h(r \otimes b)^{**} = P^{**} \otimes C_1$, and $C_2^* = h_p(h(r \otimes b)^* \| T_{U*})$. Since the computed result C_2^{**} equals the received C_2^*, S accepts the attacker's login request.

   This attack is possible because each user sends her ID in the login request message. It is obvious that the legal but malicious user, who knows the permanent secret key x, can easily impersonate any user to login S at any time.

Server spoofing attack

A legal but malicious user can impersonate a server S performing the following process:

1. Intercepts the U's login request message (ID, C_1, C_2, T_U)
2. Computes $P^* = h(ID \otimes x)$, $h(r \otimes b)^* = P \otimes C_1$, and $C_3 = h_p(h(r \otimes b)^* \otimes T_{S^*} \parallel P^*)$ where T_{S^*} denotes attacker's current timestamp
3. Sends (T_{S^*}, C_3) to U

Upon receiving the message (T_{S^*}, C_3), U computes and verifies C_3. Because the attacker used the correct secret key x and $h(r \otimes b)$, U thinks that the message send by S is correct.

User's anonymity

Chen et al.'s scheme does not preserve the anonymity of U. In the verification phase, each U sends (ID, C_1, C_2, T_U) to S over insecure channel. In this case, the privacy of U is not preserve because an attacker can eavesdrop the communication parties involve in the authentication process and can easily analyze the transaction being performed by U.

Our proposed scheme

The scheme consists of the following phases: mutual authentication, no verification table, session key agreement, single registration and update password securely. Moreover, the scheme achieves the security characteristics described in [42, 43].

Registration phase

When U desires to be registered by S, U and S carry out the following process:

1. U chooses her ID and PW
2. U sends (ID, PW) to S through a secure channel
3. S performs the equations (12), (13), (14), and (15):

$$N = h(ID \otimes x \otimes y) \quad (12)$$

$$P = h(ID \otimes x \otimes y) \otimes x \otimes y \quad (13)$$

$$R = h(ID) \otimes h(PW) \otimes h(x) \otimes h(y) \otimes h(P) \quad (14)$$

Generates a random value b

$$V = h_p(h(ID \otimes b \otimes PW)) \quad (15)$$

4. S stores b, N, R, V, $h()$, and $h_p()$ in U's smart card
5. S sends the smart card to U through a secure channel

Login phase

When U desires to get access to S, U carries out the following process:

1. U inserts her smart card into the smart card reader, and keys her ID and PW
2. U's smart card performs the following operations: $V^* = h_p(h(ID \otimes b \otimes PW))$ and checks whether V^* ?= V holds or not. If not, the smart card terminates this session. In other case, U's smart card performs the equations (16), (17) and (18):

$$C_1 = h(ID \otimes x \otimes y) \otimes h(T_U) \quad (16)$$

$$h(x) \otimes h(y) \otimes h(P) = h(ID) \otimes h(PW) \otimes R \quad (17)$$

where T_U denotes U's current timestamp

$$C_2 = h_p(h(h(x) \otimes h(y) \otimes h(P) \otimes h(T_U))) \quad (18)$$

3. U's smart card sends the login request message (C_1, C_2, T_U) to S

Verification phase

After S receives U's login request message, S carries out the following process:

1. If $(T_S - T_U) > \Delta T$, where denotes the expected valid time interval for transmission delay,

then S rejects the login request; in other case, S continues with the process

2. S performs the equations (19), (13) and (18):

$$h(ID \otimes x \otimes y)^* = C_1 \otimes h(T_U) \quad (19)$$

$$P^* = h(ID \otimes x \otimes y)^* \otimes x \otimes y \quad (13)$$

$$C_2^* = h_p(h(h(x)^* \otimes h(y)^* \otimes h(P)^* \otimes h(T_U))) \quad (18)$$

3. If C_2^* is equal to the received C_2, S accepts U's login request and performs the equations (20), (21) and (22):

$$C_3 = h_p(h(h(x)^* \otimes h(y)^* \otimes h(P)^* \otimes h(T_U) \otimes h(T_S))) \quad (20)$$

where T_S denotes S's current timestamp

$$SK = h(h(r) \otimes h(T_U) \otimes h(T_S)) \quad (21)$$

where r is a random number generated by S

$$C_4 = C_3 \otimes SK \quad (22)$$

4. S sends (T_S, C_4) to U

Upon receiving the message (T_S, C_4), U carries out the following process:

5. U Verifies either T_S is invalid or $T_S = T_U$
6. If the verification process of T_S is correct, U's smart card computes the equation (20):

$$C_3^* = h_p(h(h(x) \otimes h(y) \otimes h(P) \otimes h(T_U) \otimes h(T_S))) \quad (20)$$

7. If C_3^* is equal to the received C_3, U successfully authenticates S
8. U obtains the session key SK computing the equation (23):

$$SK = C_3 \otimes C_4 \quad (23)$$

Password change phase

When U desires to change PW, U carries out the following process:

1. U inserts its smart card into the smart card reader, keys ID and PW, and requests to change password
2. U's smart card computes $V^* = h_p(h(ID \otimes b \otimes PW))$ and checks whether V^* ?= V holds or not. If not, the smart card terminates this session. In other case, U chooses new password PW_{new}
3. U's smart card compute $R_{new} = h(ID) \otimes h(PW_{new}) \otimes h(x) \otimes h(y) \otimes h(P)$ and $V_{new} = h_p(h(ID \otimes b \otimes PW_{new}))$, and then replaces R, V with R_{new}, V_{new}, respectively.

Security analysis of our scheme

In order to prove that the proposed scheme can overcome the security weaknesses found in [28], a security analysis is presented.

Off-line secret key guessing attack

The security of the proposed scheme is more robust than [28] because the attacker needs to guess a candidate x^* and y^* to satisfy $P = h(ID \otimes x \otimes y) \otimes x \otimes y$ and $h(x) \otimes h(y) \otimes h(P)$.

Impersonation attack

Suppose that a legal but malicious user intercepts a login request message (C_1, C_2, T_U) of the victim and it attempts to impersonate U to login S at time T_V $(> T_U)$. The attacker cannot obtain U's ID and $P = h(ID \otimes x \otimes y) \otimes x \otimes y$ from C_1, C_2. Moreover, if the attacker obtains the victim's smart card, it obtains $N = h(ID \otimes x \otimes y)$, $R = h(ID) \otimes h(PW) \otimes h(x) \otimes h(y) \otimes h(P)$, $V = h_p(h(ID \otimes b \otimes PW))$, and b. Unfortunately to the intruder, nobody can extract sensitive information from N, R or V without the knowledge of the correct ID and PW. For that reasons, an impersonation attack will fail in the step 3 of the verification phase.

Server spoofing attack

A legal but malicious user cannot impersonate a server S. If an attacker intercepts the U's login request message (C_1, C_2, T_U), it cannot computes a valid C_3.

User's anonymity

In this scheme, the anonymity of *U* is guaranteed because the login request message contains a dynamic ID. In this case, the privacy of *U* is preserve because until an attacker can eavesdrop the communication parties involve in the authentication process, it cannot know the identity of *U*, achieving the main contribution of the scheme proposed in [19].

Comparison with related works

A security comparison between the proposed scheme and related works [19, 21, 28, 38] is presented. The comparison included the security characteristics described in [42, 43]. All comparisons between our proposed scheme and related works are described in table 1.

Table 1 Comparison between our scheme and related works

Security characteristics	*[19]*	*[21]*	*[28]*	*[38]*	*Our scheme*
Mutual authentication	No	Yes	Yes	Yes	Yes
Session key agreement	No	No	Yes	Yes	Yes
Single registration	Yes	Yes	Yes	Yes	Yes
Update password securely	Yes	Yes	Yes	Yes	Yes
User's anonymity	Yes	No	No	No	Yes
Without verification table	Yes	Yes	Yes	No	Yes

Table 1 shows that the scheme proposed in [19] does not provide mutual authentication, making the scheme unfeasible for practical implementation. Nowadays, a remote user authentication must contain this security characteristic. Moreover, table 1 shows that the schemes proposed in [19,21] do not establish a session key between the user and the server. Furthermore, table 1 shows that the schemes proposed in [21, 28, 38] do not keep the user's anonymity against an eavesdroppers. This means that these schemes do not keep the merits described in [19]. Additionally, table 1 shows that the scheme proposed in [38] requires that the server maintains a verification table for storing information about the smart card during the registration phase [38].

On the other hand, the proposed scheme achieved every security characteristic which a secure remote user authentication scheme should provide.

Conclusions

The security of [28] was analyzed in this paper. Although the authors claimed that their scheme can resist very well known attacks, it cannot resist off-line secret key guessing attack, impersonation attack, and server spoofing attack. In order to overcome all the security vulnerabilities found in [28], an enhancement scheme of [28] is proposed. The security analysis of the proposed scheme demonstrated that it can resist very well known attacks and security comparison between the proposed scheme and related works demonstrated that the proposed scheme achieves all the security characteristics described in [42, 43], making it more secure.

Acknowledgement

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions. This research was supported by The Mexican Teacher-Improvement Program (PROMEP), under the project number PROMEP/103.5/12/4528.

References

1. L. Lamport. "Password authentication with insecure communication". *Communications of the ACM*. Vol. 24. 1981. pp. 770-772.
2. R. Rivest. *RFC 1321 - the MD5 message-disgest algorithm*. IETF Working Group. 1992. Available on: http://www.ietf.org/rfc/rfc1321.txt. Accessed: 4 Feb. 2013.
3. NIST. *Secure Hash Standard (SHA), FIPS PUB 180-1*. 1995, National Institute of Standards and Technology. Available on: http://www.itl.nist.gov/fipspubs/fip180-1.htm. Accessed: 4 Feb. 2013.
4. C. Chang, T. Wu. "Remote password authentication with smart cards". *IEE Proceedings-E*. Vol. 138. 1991. pp. 165-168.
5. M. Hwang, L. Li. "A new remote user authentication scheme using smart card". *IEEE Transactions on Consumer Electronics*. Vol. 46. 2000. pp. 28-30.
6. T. Hwang, Y. Chen, C. Laih. *Non-interactive password authentication without password tables*. In IEEE Region 10 Conference on Computer and Communication System. Hong Kong, China. 1990. pp. 429-431.
7. C. Chang, T. Wu. *A password authentication scheme without verification tables*. In 8th IASTED International Symposium of Applied Informatics. Innsbruck, Austria. 1990. pp. 202-204.
8. T. Wu, H. Sung. "Authenticating passwords over an insecure channel". *Computer & Security*. Vol. 15. 1996. pp. 431-439.
9. W. Yang, S. Shieh. "Password Authentication Schemes with Smart Cards". *Computers & Security*. Vol. 18. 1999. pp. 727-733.
10. H. Sun. "An efficient remote use authentication scheme using smart cards". *IEEE Transactions on Consumer Electronics*. Vol. 46. 2000. pp. 958-961.
11. M. Sandirigama, A. Shimizu, M. Noda. "Simple and secure pass-word authentication protocol (SAS)". *IEICE Transactions on Communications*. Vol. 6. 2000. pp. 1363-1365.
12. C. Lee, M. Hwang, W. Yang. "A flexible remote user authentication scheme using smart cards". *ACM Operating Systems Review*. Vol. 36. 2002. pp. 46-52.
13. H. Chien, J. Jan, Y. Tseng. "An efficient and practical solution to remote authentication: smart card". *Computer & Security*. Vol. 21. 2002. pp. 372-375.
14. Y. Tang, M. Hwang, C. Lee. "A simple remote user authentication scheme". *Mathematical and Computer Modeling*. Vol. 36. 2002. pp. 103-107.
15. C. Lee, L. Li, M. Hwang. "A remote user authentication scheme using hash functions". *ACM SIGOPS Operating Systems Review*. Vol. 36. 2002. pp. 23-29.
16. J. Shen, C. Lin, M. Hwang. "A modified remote user authentication scheme using smart cards". *IEEE Transactions on Consumer Electronics*. Vol. 29. 2003. pp. 414-416.
17. W. Ku, S. Chen. "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards". *IEEE Transactions on Consumer Electronics*. Vol. 50. 2004. pp. 204-207.
18. E. Yoon, E. Ryu, K. Yoo. "Further improvement of an efficient password based remote user authentication scheme using smart cards". *IEEE Transactions on Consumer Electronics*. Vol. 50. 2004. pp. 612-614.
19. M. Das, A. Saxena, V. Gulati. "A Dynamic ID-based remote user authentication scheme". *IEEE Transactions on Consumer Electronics*. Vol. 50. 2004. pp. 629-631.
20. W. Ku, S. Chen, "Impersonation attack on a dynamic ID based remote user authentication using smartcards". *IEICE Transactions on Communications*. Vol. E88-B. 2004. pp. 2165-2167.
21. Y. Wang, J. Liu, F. Xiao, J. Dan. "A more efficient and secure dynamic ID-based remote user authentication scheme". *Computer Communications*. Vol. 32. 2009. pp. 583-585.
22. A. Awasthi. "Comment on A Dynamic ID-based remote user authentication scheme". *Transaction on Cryptology*. Vol. 1. 2004. pp. 15-16.
23. I. Liao, C. Lee, M. Hwang. *Security enhancement for a dynamic ID-based remote user authentication Scheme*. in International Conference on Next Generation Web Services Practices. Seoul, South Korea. 2005. pp. 1-4.
24. L. Hu, X. Niu, Y. Yang. "Weaknesses and improvements of a remote user authentication scheme using smart cards". *The Journal of China Universities of Posts and Telecommunications*. Vol. 14. 2007. pp. 91-94.
25. Y. Liou, J. Lin, S. Wang. *A New Dynamic ID-Based Remote User Authentication Scheme using Smart Cards*. In 16th Information Security Conference. Taichung, Taiwan. 2006. pp. 198-205.

26. M. Ahmed, D. Lakshmi, S. Sattar. "Cryptanalysis of a more efficient and secure dynamic ID-based remote user authentication scheme". *International Journal of Network Security & Its Applications*. Vol. 1. 2009. pp. 32-37.

27. S. Kim, M. Chung, "More secure remote user authentication scheme". *Computer Communications*. Vol. 32. 2009. pp. 1018-1021.

28. T. Chen, H. Hsiang, W. Shih. "Security enhancement on an improvement on two remote user authentication schemes using smart cards". *Future Generation Computer Systems*. Vol. 27. 2011. pp. 377-380.

29. E. Yoon, K. Yoo. "Improving the dynamic ID-based remote mutual authentication scheme". *On the Move to Meaningful Internet Systems.* Vol. LNCS 4277. 2006. pp. 499-507.

30. X. Wang, W. Zhang, J. Zhang, M. Khan. "Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards". *Computer Standards & Interfaces*. Vol. 29. 2007. pp. 507-512.

31. M. Misbahuddin, C. Bindu. "Cryptanalysis of Liao-Lee-Hwang's dynamic ID scheme". *International Journal of Network Security*. Vol. 6. 2008. pp. 211-213.

32. Y. Lee, G. Chang, W. Kuo, J. Chu. *Improvement on the dynamic ID-based remote user authentication scheme*. In 7th International Conference on Machine Learning and Cybernetics. Kunming, China. 2008. pp. 3283-3287.

33. S. Sood, A. Sarje, K. Singh. *An Improvement of Liao et al.'s Authentication Scheme using Smart Cards*. In IEEE 2nd International Advance Computing Conference. Patiala, India. 2010. pp. 240-245.

34. S. Sood, A. Sarje, K. Singh. *An improvement of Wang et al.'s authentication scheme using smart cards*. In National Conference on Communications. Chennai, India. 2010. pp. 29-31.

35. R. Martínez, F. Rico, C. Satizabal, J. Pomykala. *Improvement of the dynamic ID-based remote user authentication scheme*. In International Conference on Information Society. London, UK. 2010. pp. 199-208.

36. M. Khan, S. Kim, K. Alghathbar. "Cryptanalysis and security enhancement of a more efficient & secure dynamic ID-based remote user authentication scheme". *Computer Communications*. Vol. 34. 2011. pp. 305-309.

37. S. Sood. "Secure dynamic identity-based authentication scheme using smart cards". *Information Security Journal: A Global Perspective*. Vol. 20. 2011. pp. 67-77.

38. F. Wen, X. Li. "An improved dynamic ID-based remote user authentication with key agreement scheme". *Computers and Electrical Engineering*. Vol. 38. 2012. pp. 381-387.

39. R. Martínez, F. Rico, C. Satizabal, J. Pomykala. "Efficient remote user authentication scheme using smart cards". *International Journal of Internet Technology and Secured Transactions*. Vol. 3. 2011. pp. 407-418.

40. Y. Chang, H. Chang. *Security of dynamic ID-based remote user authentication scheme.* In 5th International Joint Conference on INC, IMS and IDC. Seoul, South Korea. 2009. pp. 2108-2110.

41. K. Yeh, C. Su, N. Lo, Y. Li, Y. Hung. "Two robust remote user authentication protocols using smart cards". *The Journal of Systems and Software*. Vol. 83. 2010. pp. 2556-2565.

42. R. Madhusudhan, R. Mittal, "Dynamic ID-based remote user password authentication schemes using smart cards: A review". *Journal of Network and Computer Applications*. Vol. 35. 2012. pp. 1235-1248.

43. R. Wang, W. Juang, C. Lei. "Robust authentication and key agreement scheme preserving the privacy of secret key". *Computer Communications*. Vol. 34. 2011. pp. 274-280.