IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. IV (Jan. 2014), PP 91-97
www.iosrjournals.org

Comparative Analysis of Smart Card Authentication Schemes

Toshi jain
(Oriental Institute of Science & Technology, Bhopal, INDIA)

Abstract: *Various kinds of authentication schemes have been deployed to secure the information or resources from unauthorized access. In these schemes, server maintains a verification table which is vulnerable to a variety of attacks. To withstand the possible attacks for verification table, smart card based authentication scheme has been proposed as an alternative solution. Smart card is a small, tamper-resistant device providing users with a convenient storage and processing capability, it is widely used for a range of applications such as remote user login, online banking, ID verification, access control and e-commerce etc. This article gives comparative analysis of major smart card authentication schemes for single server as well as multi-server environment.*

Keywords: *Denial-of-Service attack, denning-sacco attack, insider attack, perfect forward secrecy, user anonymity.*

I. Introduction

With the popularity of computer networks all over the world, a lot of network services are provided by remote servers. To access these services, traditional remote user authentication is usually a convenient and simple way to validate the user's legitimacy. Authentication is the basic requirement before the user avail the server through computer networks as it prevents unauthorized access. It is used to verify or validate the identity of a user prior to access the resources. In conventional password based authentication schemes, server maintains password table or verification table which contains user identity (ID) and password (PW) for all the registered users; it is used to authenticate the legitimate user. Every user has an ID and PW. Whenever a user wants to access resources from a server, user submits ID and PW to pass the authentication phase. The server verifies the PW corresponding to the ID from verification table stored in the server. If the submitted password matches the one stored in the verification table then server authenticates the user. However, there is a threat 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. In addition, if an intruder breaks into the server; the contents of the verification table can be easily modified or stolen. One of the solutions to cope with this problem is to encode the password using hash function then store the resultant test pattern in a verification table [1]. In this approach, size of the verification table is directly proportional to the number of users. It means that the size of the verification table increases as the number of users increases. Maintaining such an enormous verification table increases burden to the server. To resist all possible attacks on the verification tables, smart card based password authentication scheme 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.

The rest of the paper is organized as follows. Possible attacks and threats over the smart card based authentication schemes are described in section 2. Section 3 explores major contributions in the field of single server as well as multi-server smart card authentication. A comparison of these authentication schemes is investigated in section 4. Finally, section 5 concludes the paper.

II. Possible Attacks on Smart Card based Authentication Schemes

This section describes different types of attacks possible for smart card based authentication and these have to consider before designing a smart card authentication scheme.

1.1 Impersonation Attack

It is defined as the attack in which an attacker attempts to modify the intercepted messages transmitted between user and the server to masquerade the legal user and login to the server.

1.2 Offline Password Guessing Attack

In this, the attackers attempt to determine whether each of their guessed passwords is correct or not from the intercepted messages transmitted between user and the server. If the user's password is weak, an attacker has enough information to verify whether guessed password is correct or not. If it is true, then the attack is successful.

1.3 Online Password Guessing Attack

In this, an adversary tries to use guessed passwords iteratively to pass the authentication online. The intruder randomly guesses a password and creates a forged login request. If this login request is accepted by the server, then the intruder successfully impersonates a valid user to login server and the guessed password is user's password. This attack can be restricted by limiting the number of attempts.

1.4 Parallel Session Attack

It is defined as the attack in which the adversary eavesdrops the messages transmitted between the user and the server during mutual authentication and sends it back as a valid login request to the server.

1.5 Reflection Attack

In reflection attack, when a user sends a login request to server, an adversary eavesdrops the message and sends it (or a modified version of the message) back to the user to masquerade as the legitimate server. The reflection and parallel session attacks are possible due to the transmission of similar messages.

1.6 Insider Attack

During the registration phase, user's password is revealed to server via a secure channel. An insider of server obtains user's password and then impersonates the legal user to access other servers if same password is used to access several servers.

1.7 Attack on Perfect Forward Secrecy

A security protocol with perfect forward secrecy assures that even if one long-term key is compromised, it does not reveal any session keys used before.

1.8 Denning-Sacco Attack

It is an action where an attacker captures a session key from an eavesdropped session and uses the key either to impersonate the user or mount a dictionary attack on the user's password.

1.9 Smart Card Stolen Attack

When a smart card is lost or stolen, unauthorized user who obtains the smart card can guess the password of the user by using password guessing attacks or impersonate the user to login into the server. An adversary who steals the smart card can obtain the secret information stored in the stolen smart card by monitoring the power consumption or by analyzing the revealed information.

1.10Man-in-the-Middle Attack

It is a form of active eavesdropping in which the attacker sits between the server and user by making independent connections between them. The messages which are exchanged between the user and the server are intercepted by an attacker without the knowledge of user and server.

1.11Denial-of-Service Attack

The Denial-of-Service attack prevents/inhibits the use of network resources and communication facilities. For example, an adversary sends invalid login requests continuously to make the server busy. The adversary continuously does the same thing to overload the server which restrains the server accessibility for the valid users.

1.12 Replay Attack

The replay attack is one in which an attacker re-submits the intercepted login request to mimic as genuine user.

III. NOTEWORTHY CONTRIBUTION

III.1 Single Server Authentication Schemes

In a single server environment, a server is responsible for providing services to all the authorized remote users. In this direction, many attractive authentication schemes using smart cards have been proposed during the last decade [2, 4, 6-8, 10-15, 17, 18, 20-29]. 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 is secure against replay attack. However, it is vulnerable to impersonation attack [3]. Further improvement was given [4] which was also cryptanalyzed [5]. Modified authentication scheme was proposed to withstand impersonation attack in which login request parameters are computed from S_{ID} instead of ID [6]. Additional improvement was proposed in which S_{ID} is computed instead of ID, its login request contents are ($S_{ID} \| C_{ID}$, C_1, C_2, T_1) [7], where $C_{ID} = C_K(S_{ID})$.

A remote user authentication scheme using one-way hash function was proposed [8], its major drawbacks are a) Password is issued by the server which results the user not to choose and change the password freely. b) No mutual authentication. In addition, it has been pointed out that the scheme is vulnerable to offline and online password guessing attacks [9]. The online password guessing attack can be restricted by limiting the number of attempts. To overcome these limitations, a remote user authentication scheme using one-way hash function was proposed [10]. They claimed that their scheme does not require any password or verification table in the server and legal user could choose password without the help of the server. Moreover, it provides mutual authentication between the user and the server. However, it was pointed out that the scheme is vulnerable to parallel session attack [9]. To resist the parallel session attack, a modified scheme was also proposed [11]. Although, it was pointed out that impersonation attack and reflection attack are possible; it does not provide user anonymity [12]. The reflection and parallel session attacks are possible due to the transmission of similar messages. To conquer these weaknesses, further improvement was also proposed [12]. The scheme does not solve the time synchronization problem and server maintains an extra database for each user. To withstand insider attack and reflection attack, an improvement over the scheme [10] was proposed [13]. In addition to this, the scheme [13] allows users to change their password freely through password change phase. It was proved that the scheme is weak against parallel session attack, insecure password change phase and then further improvement has been proposed [14]. It was pointed out that the scheme is vulnerable to guessing attack, denial-of-service attack and forgery attack [15]. To overcome these drawbacks, an improved scheme was proposed which was also cryptanalyzed [16]. Further, they claimed that the scheme has guessing attack, denning-sacco attack and inadequacy to provide perfect forward secrecy.

All the schemes that use time stamp discussed so far do not solve the time synchronization problem. Nonce based scheme presented in [17] overcomes the time synchronization problem. It inherits all the previous advantages with additional feature such as session key generation agreed by the user and the server. Security flaws in this scheme are: a) It is susceptible to insider attack. b) User is not allowed to change their password freely. c) It uses symmetric encryption and decryption which is inefficient for low computational powered smart cards. Another nonce-based scheme was proposed to solve the serious time synchronization problem [18]. It encompasses all the previous features with an additional characteristic that uses one way hash function to reduce the computational cost. However, it is exposed to impersonation attack, offline password guessing attack, denial-of-service attack and man-in-the-middle attack [19].

An ID based scheme using RSA cryptosystem has been proposed [20]. However, it exhibit impersonation attack [21]. Further improvement has been proposed [22] which has all the merits of the previous scheme with an added trait of mutual authentication. It has been found that the scheme does not resist impersonation attack [23]. A user friendly authentication scheme using one way hash function was proposed [24]. It was proved that the scheme is weak against impersonation attack and then further improvement was also proposed [25]. It was pointed out that the scheme is vulnerable to guessing attack, forgery attack; to overcome these weaknesses, an improved scheme was also proposed [26]. However, due to the symmetric structure of communicating messages, this scheme does not resist reflection attack and parallel session attack.

A dynamic ID-based remote user authentication scheme using one way hash function has been proposed [27]. It was claimed that the scheme allows the users to choose and change their passwords freely, secure against ID-theft, and resists reply attack, forgery attack, guessing attack, insider attack and stolen verifier attack. However, it was proved that the scheme is insecure against guessing attack and does not provide mutual authentication [28]. To defeat these flaws, a new scheme was also suggested which was then cryptanalyzed through impersonation attack and proposed an improved scheme [29]. 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. It has been proved that the scheme [27] does not provide mutual authentication and it is password independent; to overcome these imperfections, an enhanced scheme was also proposed [30]. It was pointed out that the scheme does not resist insider attack, does not provide users to choose the password, session key establishment and does not preserve user anonymity [31]. An improved scheme was also proposed to overcome these weaknesses. Major drawbacks in this scheme are a) Server has to maintain extra table for the value of N corresponding to every user, where N denotes the number of times a user U_i registers at the server. b) Slow wrong password detection.

III.2 Multi-server Authentication Schemes

If a user wishes to access several network services, the user must register its identity and password in different servers and maintain several user IDs and PWs. To handle this problem, various schemes have been proposed. These authentication schemes enable users to obtain service from multiple servers without separately registering with each server. First authentication scheme for multi-server architecture using neural networks has been proposed [32]. In this, users can freely choose their passwords. The major drawback of this approach is that it spends long time on training neural networks [33]. A new scheme based on ElGamal digital signature and simple geometric properties on the Euclidean plane has also been proposed. The major advantage of this scheme is that users can freely choose and change their passwords. However, it does not resist impersonation attack [34]. Also, in this scheme [33], every user must have a large amount of memory to store the public parameters for authentication which is unrealistic for small storage smart card based applications. To overcome these weaknesses, a nonce based scheme using one-way hash function and symmetric cryptosystem was proposed [35]. It has all the previous advantages as well as server and user authenticate each other and generate a session key agreed between them. However, it exhibits insider attack and does not provide forward secrecy [36]. Further improvement was also proposed [37]. They claimed that their scheme provides mutual authentication between the remote server and the user, resists stolen-verified attack, server spoofing attack, smart card loss attack, replay attack and provides forward secrecy.

A dynamic ID based remote user authentication scheme has been given to provide user anonymity using one way hash function [38]. It has been proved that the scheme fails to provide forward secrecy [39]. It has been pointed out that the scheme [38] does not resist insider attack, impersonation attack, server spoofing attack, registration centre spoofing attack, fails to provide mutual authentication and further improvement has been proposed [40]. A nonce based scheme using one way hash function has been given [41]. It has been proved that the scheme fails to provide perfect forward secrecy, is susceptible to denning-sacco attack, server spoofing attack and an improved scheme has been proposed [42]. Sood et al. [43] also showed that Hsiang-Shih's improved scheme [40] fails to provide security against replay attack, impersonation attack, stolen smart card attack and has incorrect password change phase. Further, they suggested an improved scheme and claimed that their scheme withstands replay attack, impersonation attack, stolen smart card attack, online and online dictionary attack, parallel session attack, MITM attack, message modification attack and DoS attack. But, it shows in- adequacy to provide security against stolen smart card attack and leak of verifier attack [44, 45]. Moreover, it has incorrect authentication and session key agreement phase [45]. Recently, Wang and Ma [46] 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 [47]. 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. [48] also proposed their scheme but involvement of RC during verification makes it inefficient practically

.

IV. COMPARISON OF MAJOR SMART CARD BASED AUTHENTICATION SCHEMES

This section provides a comparison result for both single server and multi sever smart card based authentication scheme. Table I shows comparative results in terms of computational complexity for single server authentication scheme. Table II explores comparative analysis for 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
Ex	:	Modular Exponentiation
En	:	Symmetric Encryption
De	:	Symmetric Decryption
(N)	:	Nonce based scheme
*	:	Includes session key generation
(T)	:	Timestamp based scheme

TABLE I
COMPARISON RESULTS FOR SINGLE SERVER SMART CARD BASED AUTHENTICATION SCHEMES IN TERMS OF COMPUTATIONAL COST

Authentication Schemes	Registration Phase		Login Phase		Authentication Phase	
	User	Server	User	Server	User	Server
Hwang et al.'s scheme	-	1Ex	1H + 3Ex	-	-	1H + 3Ex
Shen et al.'s scheme	-	1Ex	1H + 3Ex	-	-	1H + 3Ex
Awasthi et al.'s scheme	-	1Ex	1H + 3Ex	-	-	1H + 3Ex
Kumar's scheme	-	1Ex	1H + 3Ex	-	-	1H + 3Ex
Sun's scheme	-	1H	IH	-	-	2H
Chien et al.'s scheme	-	1H	2H	-	1H	3H
Lee et al.'s scheme	-	1H	2H	-	2H	4H
Sood et al.'s scheme*	4H	3H	8H	-	2H	6H
Ku et al.'s scheme	1H	1H	2H	-	1H	3H
Yoon et al.'s scheme	1H	1H	2H	-	1H	3H
Wang et al.'s scheme*	IH	2H	4H	-	1H	3H
Juang's scheme*	-	1H	1H + 1En	-	1H + 1En + 1De	3H + 1En + 2De
Liaw et al.'s scheme	-	1H	1H	-	1De	2H + 1En
Yang et al.'s scheme (T)	-	2Ex	1H + 2Ex	-	-	1H + 2Ex
Yang et al.'s scheme (N)	-	2Ex	2Ex	1H	-	2Ex
Shen et al.'s scheme	-	1H + 2Ex	1H + 2Ex	-	1H + 1Ex	3H + 3Ex
Wu et al.'s scheme	-	2H + 1Ex	2H + 1Ex	-	-	1H
Lee et al.'s scheme	-	2H + 1Ex	2H + 1Ex	-	-	2H
Marko et al.'s scheme	-	3H + 1Ex	4H + 1Ex	-	1H	3H
Das et al.'s scheme	-	2H	4H	-	-	3H
Liao et al.'s scheme	1H	1H	4H	-	1H	4H
Xie et al.'s scheme	1H	2H	4H	-	1H	5H
Wang et al.'s scheme	-	2H	2H	-	1H	3H
Khan's scheme*	1H	1H	3H	-	2H	5H

TABLE II
COMPARISON OF SMART CARD BASED AUTHENTICATION SCHEMES IN TERMS OF COMPUTATIONAL COMPLEXITY WITH MULTI-SERVER

Authentication Schemes	User Registration	Server Registration	Login Phase	Authentication Phase
Lin et al.'s scheme	5Ex	1Ex	4Ex	6Ex
Juang's scheme*	2H + 1En	1H	2H + 1En	3H + 2En + 4De
Chang et al.'s scheme*	2H	-	2H + 1En	6H + 2En + 3De
Liao et al.'s scheme*	5H	-	6H	10H
Hsiang et al.'s scheme*	6H	1H	7H	16H
Tsai's scheme*	2H	1H	1H	17H
Zhu et al.'s scheme*	2H	1H	3H + 1Ex	20H + 7Ex

V. CONCLUSION

Security and efficiency are the main factors for any authentication scheme from the user's point of view. In this context, several smart card based remote user authentication schemes have been proposed for single server as well as multi-server environment. This paper describes a comparative analysis of major smart card authentication schemes in terms of their computational efficiencies. In addition, it explains possible attacks and threats that have to be considered while designing an authentication scheme. This effort assists the researchers to work in different directions towards design and development of secure and efficient smart card authentication scheme.

ACKNOWLEDGEMENT

I would like to Thank **Dr. Ateet Bhalla** for his kind support, discussions with him greatly inspired me for some worthful comment.

REFERENCES

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

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

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

[4] J. J. Shen, C. W. Lin and M. S. Hwang, "A modified remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, vol. 49, no. 2, 2003, pp. 414-416.

[5] Kai-Chi Leung, L.M. Cheng, Anthony S. Fong, and Chi-Kwong Chan, "Cryptanalysis of a modified remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, vol. 49, no. 4, 2003, pp. 1243-1245.

[6] A. K. Awasthi and S. Lal, "An enhanced remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, vol. 50, no. 2, 2004, pp. 583-586.

[7] Manoj Kumar, "New remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, vol. 50, no. 2, 2004, pp. 597-600.

[8] H.M. Sun, "An efficient remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, vol. 46, no. 4, 2000, pp. 958-961.

[9] Chien-Lung Hsu, "Security of two remote user authentication schemes using smart cards", IEEE Transactions on Consumer Electronics, vol. 49, no. 4, 2003, pp. 1196-1198.

[10] Hung-Yu Chien, Jinn-Ke Jan and Yuh-Min Tseng, "An efficient and practical solution to remote authentication: smart card", Computers & Security, vol. 21, no. 4, 2002, pp. 372-375.

[11] Sung-Woon Lee, Hyun-Sung Kim and Kee-Young Yoo, "Improvement of Chien et al.'s remote user authentication scheme using smart cards", Computer Standards & Interfaces, vol. 27, no. 2, 2005, pp. 181-183.

[12] Sandeep K. Sood, Anil K.Sarje and Kuldip Singh, "Secure dynamic identity-based remote user authentication scheme", Distributed Computing and Internet Technology, Lecture Notes in Computer Science, vol. 5966, 2010, pp. 224-235.

[13] W.C. Ku and S.M. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, vol. 50, no. 1, 2004, pp. 204–207.

[14] Eun-Jun Yoon, Eun-Kyung Ryu, and Kee-Young Yoo, "Further improvement of an efficient password based remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, vol. 50, no. 2, 2004, pp. 612-614.

[15] Xiao-Min Wang, Wen-Fang Zhang, Jia-Shu Zhang and Muhammad Khurram Khan, "Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards", Computer Standards & Interfaces, vol. 29, no. 5, 2007, pp. 507-512.

[16] Eun-Jun Yoon, Eun-Jung Lee and Kee-Young Yoo, "Cryptanalysis of Wang et al.'s remote user authentication scheme using smart cards", Fifth International Conference on Information Technology: New Generations, 2008, pp. 575 – 580.

[17] Wen-Shenq Juang, "Efficient password authenticated key agreement using smart cards", Computers & Security, vol. 23, no. 2, 2004, pp. 167-173.

[18] Horng-Twu Liaw, Jiann-Fu Lin and Wei-Chen Wu, "An efficient and complete remote user authentication scheme using smart cards", Mathematical and Computer Modelling, vol. 44, no. 1-2, 2006, pp. 223-228.

[19] Huang Kai, Ou Qingyu, Wu Xiaoping and Song Yexin, "Cryptanalysis of a remote user authentication scheme using smart cards", 5th International Conference on Wireless Communications, Networking and Mobile Computing, 2009, pp. 1-4.

[20] Wen-Her Yang and Shiuh-Pyng Shieh, "Password authentication schemes with smart cards", Computers & Security, vol. 18, no. 8, 1999, pp. 727-733.

[21] C. K. Chan and L. M. Cheng, "Cryptanalysis of timestamp-based password authentication scheme", Computer & Security, vol. 21, no. 1, 2002, pp. 74-76.

[22] Jau-Ji Shen, Chih-Wei Lin and Min-Shiang Hwang, "Security enhancement for the timestamp-based password authentication scheme using smart cards", Computers & Security, vol. 22, no. 7, 2003, pp. 591-595.

[23] L. Yang and K. Chen, "Cryptanalysis of a timestamp-based password authentication scheme", 2004. Available: http://eprint.iacr.org/2004/040.pdf.

[24] Shyi-Tsong Wu and Bin-Chang Chieu, "A user friendly remote authentication scheme with smart cards", Computers & Security, vol. 22, no. 6, 2003, pp. 547-550.

[25] Narn-Yih Lee and Yu-Chung Chiu, "Improved remote authentication scheme with smart card", Computer Standards & Interfaces, vol. 27, no. 2, 2005, pp. 177-180.

[26] Marko Holbl and Tatjana Welzer, "Cryptanalysis and improvement of an 'improved remote authentication scheme with smart card'", Third International Conference on Availability, Reliability and Security, 2008, pp. 1301-1305.

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

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

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

[30] Yan-yan Wang, Jia-yong Liu, Feng-xia Xiao and Jing Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme", Computer Communications, vol. 32, no. 4, 2009, pp. 583-585.

[31] Muhammad Khurram Khan, "Enhancing the security of a 'More efficient & secure dynamic ID-based remote user authentication scheme'", Third International Conference on Network and System Security, 2009, pp. 420–424.

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

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

[34] X. Cao and S. Zhong, "Breaking a remote user authentication scheme for multiserver architecture", IEEE Communications Letters, vol. 10, no. 8, 2006, pp. 580-581.

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

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

[37] C.C. Chang and J.S. Lee, "An efficient and secure multi-server password authentication scheme using smart cards", Proceedings of International Conference on Cyberworlds, no. 18-20, 2004, pp. 417-422.

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

[39] Te-Yu Chen, Min-Shiang Hwang, Cheng-Chi Lee, Jinn-Ke Jan, "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, 2009, pp. 725-728.

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

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

[42] Hongfeng Zhu, Tianhua Liu and Jie Liu, "Robust and Simple Multi-server Authentication Protocol without Verification Table", 2009 Ninth International Conference on Hybrid Intelligent Systems, 2009, pp. 51-56.

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

[44] B. L. Chen, W. C. Kuo and L. C. Wuu, "Cryptanalysis of Sood et al.'s dynamic identity based authentication protocol for multi-server architecture," International Journal of Digital Content Technology and its Applications, vol. 6, no. 4, 2012, pp. 180-187.

[45] X. Li, Y. Xiong, J. Ma and W. Wang, "An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards," Journal of Network and Computer Applications, vol. 35, no. 2, 2012, pp. 763-769.

[46] B. Wang and M. Ma, "A smart card based efficient and secured multi-server authentication scheme," Wireless Personal Communications, 2012.

[47] D. He and S. Wu, "Security flaws in a smart card based authentication scheme for multi-server environment," Wireless Personal Communications, 2012.

[48] 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.