Cryptanalysis for Secure and Efficient Smart-Card-Based Remote User Authentication Scheme for Multi-server Environment

Azeem Irshad, Muhammad Sher, Shahzad Ashraf, Shahzad faisal, Mahmood Ul Hassan

Computer Science department
International Islamic University, Islamabad
{Irshadazeem2, md.sher, shahzadas, ch_shahzad, Mahmood_iiu}@gmail.com

Abstract: Multi-server authentication is going to be an integral part of remote authentication with the passage of time. The remote authentication has been part and parcel of internet based communication. In the last decade several multi-server authentication techniques has been presented. However there is still a need of more efficient and robust techniques. Lately, Saraswathi et al., presented a multi-server authentication scheme that has been found under much vulnerability like stolen card attack, misrepresentation attack, and forward secrecy attacks. This paper presents the cryptanalysis for Saraswathi et al. scheme and shows the review analysis.

1. Introduction

Multi-server authentication is termed as overhead efficient since it minimizes the cost when a user needs to access multiple services over several servers in the network. The concept has been almost based upon single-sign-on where a single authentication relieves the user of more than one authentication with the corresponding server, but with few differences. As in multi-server the user needs to re-login at other related server, although with the same password and parameters. The remote internet authentication often entails such type of multi-server authentications, which further underscores the efficiency and robustness of these protocols.

In the last decade several multi-server authentication techniques has been presented. However there is still a need of more efficient and robust techniques. Lately, Saraswathi et al., presented a multi-server authentication scheme, that has been found under many vulnerabilities like stolen card attack, misrepresentation attack, and forward secrecy attacks. Initially, Li et al [8] presented a scheme for remote authentication using neural network. The scheme was taking much cost for its training and maintaining neural networks. Lin et al. [11] presented another multi-server authentication scheme that was based on ElGamal signature technique. Juang [2] pointed out that the scheme was not efficient for taking a large amount of memory required for storing the authentication parameters, and also presented its authentication protocol based on symmetric cryptography. However, the scheme was found exposed to man-in-the-

middle attack and password guessing attack. Besides, it could also not employ the smart card during authentication login procedure. That scheme could also not change the password if the services of Registration center are not available. Afterwards, Tsaur [16] and Tsaur et al. [17] presented an RSA cryptosystem based multi-server authentication protocol. The scheme developed the protocol without verification table, however, the scheme had to bear high computation cost, and there was no anonymity at all in the protocol. Thereafter, Chang and Lee [5] also presented a multi-server protocol based on symmetric key encryption that was found vulnerable to insider and masquerading attacks. Tsai [19] presented another scheme in this domain based on one way hash function.

The majority of these schemes were not focusing on user anonymity and were sending the user identity IDi in plaintext. For countering this, Liao and Wang [7] presented a new dynamic ID based multi-server authentication scheme, where the user ID gets changed dynamically every time the user attempts to login server. However Hsiang and Shih [1] revealed that the scheme fails to achieve mutual authentication and also suffers insider attacks and spoofing attacks. Then Liao and Wang proposed another improved version of the scheme countering the above flaws. Sood et al [20] in return revealed few more flaws in both Hsiang and Shih, and Liao and Wang schemes, for instance, replay attack, stolen card attack and masquerading attack. Sood et al also presented an improved authentication protocol after pointing these attacks out. Afterwards, Li et al, found the verifier leak attack, impersonation and stolen card attack in Sood et al, scheme, and proposed a new scheme. Xue et al. found the vulnerability of Li et al. scheme by introducing denial of service, replay and masquerading attacks, and conceive with a new protocol. Lee et al. [9] found the above scheme with masquerading and spoofing attack along with the lack of mutual authentication. Lee proposed the two schemes serially [9] and [6] to counter the above mentioned attacks and enhance security. Li et al. [15], then, found again the Lee et al. scheme suffering forgery, server spoofing attacks, and presented its own scheme. Saraswathi et al. [24] found the attacks In Li et al. scheme by removing the assumption of exposed secret knowledge h(x||y) and h(y), that earlier schemes assumed for discovering various attacks in Li et al. scheme. However Saraswathi et al. has been found under many vulnerabilities like stolen card attack, misrepresentation attack, and known secrecy attacks. The objective of our paper is to discover the vulnerability of Saraswathi et al. scheme and show cryptanalysis for the possible attacks. In section 2, the working for Saraswathi scheme has been studied. In section 3 the cryptanalysis for Saraswathi scheme has been presented, while the last section 4 concludes the findings.

2. Working and Review of Saraswathi et al. scheme

The Saraswathi et al.'s scheme [24] consists of four phases: Registration, Login, Authentication, and password modification phase, and has been shown in Figure 1. Some notations that have been used in the paper are given as under.

Ui: ith user

IDi: Identity of user Ui

PWi: Ui's password

Bi: biometric impression of Ui

Sj:The jth server

RC: Registration center

h(.): a secure hash digest function

x: Server's master key

y: A secret number generated by Registration Center

b: A random secret generated by Ui

SC: Smart Card

SK: A shared Session Key between Ui and Sj

CIDi: The randomly generated dynamic ID of Ui

||: concatenation function

⊕: XOR function

This scheme assumes one trusted RC and n number of trusted servers Sj, where j=1…..n. The Sj makes registration with RC and RC shares two parameters h(x||y) and h(y) with server using secure channel.

2.1 The Registration Phase

In this phase Ui registers with RC, while Sj has already been registered with RC. Afterwards Ui can access all Sj servers. RC performs with Ui the following steps:

1. The Ui sends IDi , Ai=h(b || PWi)by computing and assuming a random number b to RC, using a secure channel.The RC receives the IDi and Ai and computes and sends the SC towards Ui by storing Bi, Ci, Di, Ei and h(y) in it.

$$Bi=h(IDi \,||\, x)$$
$$Ci=h(IDi \,||\, h(y) \,||\, Ai)$$

$$Di=h(Bi \,||\, h(x \,||y)) \oplus Ai$$
$$Ei= Bi \oplus h\,(x \,||y)$$

2. Finally, the Ui stores b in smart card, Now the SC contains the parameters {Ci, Di, Ei, b, h(), h(y)}

2.2 The Login and Authentication Phase

1. In login phase the Ui uses the SC for getting authenticated access to Sj. For this purpose the Ui inputs its IDi and PWi and computes Ai =h(b|| PWi), and Ci*=h(IDi||h(y) ||Ai) and compares Ci* with Ci. On successful verification, the SC allows the Ui to proceed for next procedure. Now the Ui generates Ni random ineger, and computes Pij, Fi, Ali, CIDi, and M1.

$$Pij = Ei \oplus h(h(SIDj \,||\, h(y)) \,||Ni)$$
$$Fi=Di \oplus Ai$$
$$Ali=h(Ai \,||Ni)$$
$$CIDi=Ali \oplus h(Fi \,||\, SIDj \,||Ni)$$
$$M1=h(Pij \,||CIDi \,||Fi \,||Ni)$$

   Next, the Ui sends {Pij, CIDi, M1, Ni } towards Sj.

2. In the authentication phase the Sj receives parameters and computes Ei, Bi, Fi, Ali by the following computations:

$$Ei=Pij \oplus h(h(SIDj \,||\, h(y)) \,||Ni)$$
$$Bi= Ei \oplus h(x \,||\, y)$$
$$Fi =h(Bi \,||\, h(x||y))$$
$$Ali= CIDi \oplus h(Fi \,||\, SIDj \,||Ni)$$

3. Now Sj compares h(Pij ||CIDi || Fi || Ni) ?= M1. On successful verification it generates M2 and M3 and sends to Ui.

$$M2=h(Fi \,||Ali \,||Nj \,||\, SIDj)$$
$$M3=Ali \oplus Ni \oplus Nj$$

4. Ui, after receiving M2 and M3, computes Nj by performing Ali⊕Ni⊕M3. Now it verifies the messages by comparing h(Fi|| Ali||Nj||SIDj) ?=M2. On successful verification it computes M4 =h(Fi|| Ali||Ni||SIDj). Now it sends M4 towards Sj.
5. Sj compares by following computation h(Fi|| Ali||Ni||SIDj) ?= M4. If it verifies true, then it computes the session key SK as h(Fi|| Ali||Ni||Nj||SIDj), otherwise discards the message. The Ui also generates and shares the same session key SK.

$$SK = h(Fi|| Ali||Ni||Nj||SIDj)$$

2.3 Password Updating Phase

Ui changes its password by invoking this procedure, into a new password PWi^{new}. It does require any interaction with RC. The procedure has been mentioned below:

1. Ui inputs Idi and PWi after inserting SC into the card reader.
2. The SC computes Ai and Ci* by computing Ai=h(b||PWi) and Ci* =h(Idi||h(y)||Ai). It checks the equality of Ci* and Ci. The SC declines to proceed if the equality does not hold. Otherwise, Ui inputs a new password PWi^{new} along with a new random integer b^{new}.
3. Now the SC will compute the following parameters.

$$Ai^{new}=h(b^{new} \,||\, PWi^{new})$$
$$Ci^{new}=h(Idi||h(y) \,||Ai^{new})$$
$$Di^{new}=Di \oplus Ai \oplus Ai^{new}$$

4. Finally, the SC would replace Ci with Ci^{new}, Di with Di^{new} for completing the password changing process.

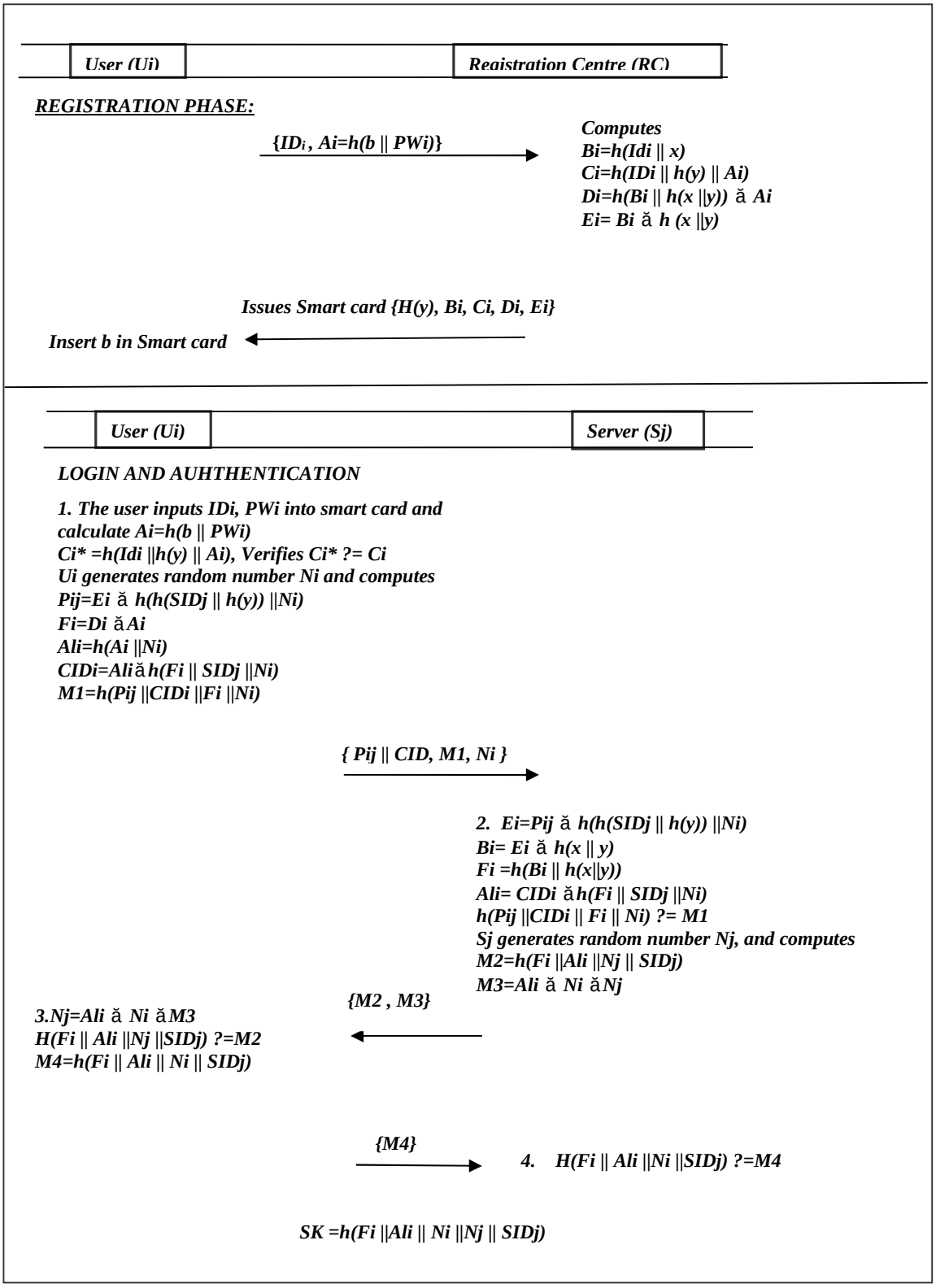

Figure 1. Saraswathi et al. model Registration, Login and Authentication phase

3. Cryptanalysis of the Saraswathi et al. scheme.

The Saraswathi et al. scheme has been vulnerable to three types of attacks i.e., insider attack, forward secrecy attack, and stolen smart card attack.

3.1 Misrepresentation/Insider Attack

The misrepresentation attacks are those attacks that are launched by an adversary to misrepresent some other participant as a valid user. The other participant is made to believe in deception that the current participating user is a valid entity.
A legal user Ui, for having access to its ownSC parameters Bi, Ci, Di, Ei etc., could easily extract h(x||y)by doing the computation h(x||y)=Ei ăBi. The h(x||y) and h(y) remains the same for all users Ui. In this scenario, if any legal user Ui turns malicious, then this malicious adversary A could launch an impersonation attack against Ui, and impersonate as Sj. The attack could be launched by adopting the following steps.

1. After receiving the message {Pij, CIDi, M1, Ni} from Ui, the adversary A, having the knowledge of SIDj, h(y), Ni, would compute Ei*, Bi*, Fi*, Ali* values.

$$Ei^* = Pij \oplus h(h(SIDj \,||\, h(y)) \,||Ni),$$
$$Bi^* = Ei^* \oplus h(x \,||\, y),$$
$$Fi^* = h(Bi^* \,||\, h(x||y)),$$
$$\text{and } Ali^* = CIDi \oplus h(Fi^* \,||\, SIDj \,||Ni)$$

2. Now Acreate M2* and M3* by doing the following computations.

$$M2^* = h(Fi^* \,||Ali^* \,||Nj \,||\, SIDj)$$
$$M3^* = Ali^* \oplus Ni \oplus Nj$$

3. A now sends {M2*, M3*} towards Ui for verification.

Ui receives the message and computes Nj* by computing Nj* = ALi⊕ Ni⊕M3* and compares the equality H(Fi || Ali ||Nj ||SIDj) ?=M2*. On successful equality check, it generates M4 as M4=h(Fi || Ali || Ni || SIDj), which is sent towards A under the guise of a server. The A now generates a valid session key SK={Fi* || Ali* || Ni || Nj || SIDj} which is exactly the same as the Ui generates on its end. In this way an adversary may launch a successful attack.

3.2 Stolen Smart Card Attack

The stolen smart card attacks are launched when the card gets stolen and any malicious user gets away with the stored parameters and uses those for its malicious purpose.
In Saraswathi et al. scheme, if the smart card gets stolen by an adversary A, then it might access all stored parameters like Bi, Ci, Di, Ei, and h(y) and could easily extract h(x||y) by doing the computation h(x||y)=Ei ăBi. In this scenario, A could launch stolen SC attack against Ui, and generate the previous session keys by adopting the following steps.

1. A stores all the previously exchanged messages { Pij, CIDi, M1, Ni, M2, M3, M4}of earlier legal communicating sessions. The session key can be established by computing SK= h(Fi || Ali || Ni || Nj || SIDj). In this scenario, the adversary having the knowledge of SIDj, h(y), Ni, would compute Ei*, Bi*, Fi*, Ali* values with the help of those stored messages.

$$Ei^*=Pij \oplus h(h(SIDj \| h(y)) \|Ni),$$
$$Bi^*= Ei^* \oplus h(x \| y),$$
$$Fi^* =h(Bi^* \| h(x\|y)),$$
$$\text{and } Ali^*= CIDi \oplus h(Fi^* \| SIDj \|Ni)$$

2. Now A gets all of the valid parameters for establishing a session key except Nj*. This will extract Nj* doing the following computation.
$$Nj^*=Ali^* \oplus Ni \oplus M3^*$$

3. In this manner, an adversary combines all of the individual elements to create all of the previous session keys by computing SK={Fi* || Ali* || Ni || Nj* || SIDj}.

3.3 Forward Secrecy Attack

The forward secrecy attacks could be launched by an adversary if the exposed private keys of legal participants lead to the calculation of previous session keys.
If we assume, the master key ‘x’ and its secret key ‘y’ gets leaked for some reason, then the adversary could recover the previous session keys from stored messages as defined in the following steps.

1. Having come to know about the secret parameters, A could easily compute the two values h(x||y) and h(y). Now the attacks could be launched in the same fashion, as we mentioned above regarding two attacks. For deriving the previous session keys A would utilize stored messages { Pij, CIDi, M1, Ni, M2, M3, M4}. As we know that, the session key can be established by computing SK= h(Fi || Ali || Ni || Nj || SIDj). In this scenario, A having the knowledge of SIDj, h(y), Ni, computes Ei*, Bi*, Fi*, Ali* values out of those stored messages.

$$Ei^*=Pij \oplus h(h(SIDj \| h(y)) \|Ni),$$
$$Bi^*= Ei^* \oplus h(x \| y),$$
$$Fi^* =h(Bi^* \| h(x\|y)),$$
$$\text{and } Ali^*= CIDi \oplus h(Fi^* \| SIDj \|Ni)$$

2. Next, A will extract Nj* by computing Nj* =Ali* ⊕ Ni ⊕ M3*, and will generate the session key by taking hash of the concatenated elements SK={Fi* || Ali* || Ni || Nj* || SIDj}.

Our cryptanalysis reveals the three ways, in which the scheme could be attacked, 1) misrepresentation attack, 2) stolen smart card attack and 3) forward secrecy attack. While, our future research work lies with the proposal for an improved and robust version of multi-server authentication scheme that covers the prevalent threats currently found in most of the schemes.

4. Conclusion

The multi-server authentication has been acknowledged as one of the chief requirements of the current internet authentication paradigm. A lot of schemes has been proposed in the last decade by the research academia. This paper studies the Saraswathi et al. scheme that is based on multi-server remote authentication. The review of Saraswathi et al and other related schemes has been presented thoroughly. The Saraswathi et al. scheme was found vulnerable to few threats, lately. Our cryptanalysis reveals the three ways, in which the scheme could be attacked, 1) misrepresentation attack, 2) stolen smart card attack and 3) forward secrecy attack. Our future research work lies with the proposal for an improved and robust

version of multi-server authentication scheme that covers the prevalent threats currently found in most of the schemes.

References

[1] H.-C. Hsiang and W.-K. Shih, “Improvement of the secure dynamicID based remote user authentication scheme for multi-server environment,”Comput. Standards Interf., vol. 31, no. 6, pp. 1118–1123,2009.

[2] W.-S. Juang, “Efficient multi-server password authenticated key agreementusing smart cards,” IEEE Trans. Consum. Electron., vol. 50, no. 1,pp. 251–255, Feb. 2004

[3] T. H. Kim, C. Kim, and I. Park, “Side channel analysis attacks using AMdemodulation on commercial smart cards with SEED,” J. Syst. Softw.,vol. 85, no. 12, pp. 2899–2908, 2012.

[4] C.-C. Chang and T.-C. Wu, “Remote password authentication with smartcards,” IEE Proc. Comput. Digit. Techn., vol. 138, no. 3, pp. 165–168,May 1991.

[5] C.-C. Chang and J.-S. Lee, “An efficient and secure multi-serverpassword authentication scheme using smart cards,” in Proc. Int. Conf.Cyberworlds, Nov. 2004, pp. 417–422.

[6] C.-C. Lee, Y.-M. Lai, and C.-T. Li, “An improved secure dynamic IDBased remote user authentication scheme for multi-server environment,”Int. J. Secur. Appl., vol. 6, no. 2, pp. 203–209, 2012.
[7] Y.-P. Liao and S.-S. Wang, “A secure dynamic ID based remote userauthentication scheme for multi-server environment,” Comput. StandardsInterf., vol. 31, no. 1, pp. 24–29, 2009.

[8] L.-H. Li, L.-C. Lin, and M.-S. Hwang, “A remote password authenticationscheme for multiserver architecture using neural networks,” IEEETrans. Neural Netw., vol. 12, no. 6, pp. 1498–1504, Nov. 2001.

[9] C.-C. Lee, T.-H. Lin, and R.-X. Chang, “A secure dynamic ID basedremote user authentication scheme for multi-server environment usingsmart cards,” Expert Syst. Appl., vol. 38, no. 11, pp. 13863–13870, 2011.

[10] L. Lamport, “Password authentication with insecure communication,”Commun. ACM, vol. 24, no. 11, pp. 770–772, 1981.

[11] I.-C. Lin, M.-S. Hwang, and L.-H. Li, “A new remote user authenticationscheme for multi-server architecture,” Future Generat. Comput. Syst.,vol. 19, no. 1, pp. 13–22, 2003.

[12] R. Madhusudhan and A. Praveen, “Weaknesses of a dynamic IDbased remote user authentication protocol for multi-server environment,”J. Comput. Commun., vol. 2, no. 4, pp. 196–200, 2014.

[13] S. Mangard, E. Oswald, and T. Popp, Power Analysis Attacks: Revealingthe Secrets of Smart Cards. Berlin, Germany: Springer-Verlag,2010.

[14] 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,” J. Netw. Comput. Appl., vol. 35, no. 2, pp. 763–769, 2012.

[15] X. Li, J. Ma, W. Wang, Y. Xiong, and J. Zhang, “A novel smart card anddynamic ID based remote user authentication scheme for multi-server environment,” Math. Comput. Model., vol. 58, nos. 1–2, pp. 85–95, 2013.

[16] W.-J. Tsaur, “A flexible user authentication scheme for multi-serverinternet services,” in Networking—ICN. Berlin, Germany: Springer-Verlag, 2001, pp. 174–183.

[17] W.-J. Tsaur, C.-C. Wu, and W.-B. Lee, “A smart card-based remotescheme for password authentication in multi-server internet services,”Comput. Standards Interf., vol. 27, no. 1, pp. 39–51, 2004.

[18] Y.-M. Tseng, T.-T. Tsai, and T.-Y. Wu, “Efficient revocable multi-receiver ID-based encryption,” Inf. Technol. Control, vol. 42, no. 2,pp. 159–169, 2013.

[19] J.-L. Tsai, “Efficient multi-server authentication scheme based on one-way hash function without verification table,” Comput. Secur.,vol. 27, nos. 3–4, pp. 115–121, 2008.

[20] S. K. Sood, A. K. Sarje, and K. Singh, “A secure dynamic identity based authentication protocol for multi-server architecture,” J. Netw. Comput.Appl., vol. 34, no. 2, pp. 609–618, 2011.

[21] D. Zhao, H. Peng, S. Li, and Y. Yang, “An efficient dynamic ID based remote user authentication scheme using self-certified public keys formulti-server environment,” arXiv preprint arXiv:1305.6350, May 2013.
[Online]. Available: http://arxiv.org/abs/1305.6350

[22] K. Xue, P. Hong, and C. Ma, “A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture,” J. Comput. Syst. Sci., vol. 80, no. 1,pp. 195–206, 2014.

[23] D. Wang and C. G. Ma. (2012). “Robust smart card based password authentication scheme against smart card security breach,” Cryptology ePrint Archive, Tech. Rep. 2012/439. [Online]. Available:http://eprint.iacr.org/2012/439.pdf

[24] S. Saraswathi, R. D. Saravanan, and Y. Palanichamy. "Secure and Efficient Smart-Card-Based Remote User Authentication Scheme for Multiserver Environment." Electrical and Computer Engineering, Canadian Journal of 38.1 (2015): 20-30.