Cryptanalysis of an Efficient Password Authentication Scheme

Chiu-Shu Pan
and Cheng-Yi Tsai
Department of Computer Science
and Information Engineering,
Asia University, Taiwan

Shyh-Chang Tsaur
Department of Electronic Engineering,
National Chin-Yi University
of Technology, Taiwan

Min-Shiang Hwang
Department of Computer Science
and Information Engineering,
Asia University, Taiwan

***Abstract*—Recently, Thandra et al. proposed an efficient password authentication scheme. Their scheme is secure, efficient, and easy to implement. However, we find some weaknesses of their scheme in this article. We will show that their scheme is vulnerable to denial of service attacks, online and offline password guessing attacks, and impersonation attacks.**

I. Introduction

One of methods to verify remote users over public Internet is a remote authentication scheme. There are three types of remote authentication schemes which have been used to verify the legitimacy of remote users. The first type is based on biometric [13], [22], [23]. The second type is based on the smart card [2], [4], [12], [15], [19], [21]. The third type is based on a password [7], [16], [24], [25]. Some authentication schemes with anonymity for wireless environments are also proposed [5], [11]. Some authentication schemes are used in Multi-server Environment [1], [3], [6], [10].

In 2016, Wei et al. proposed a remote user password authentication scheme [20]. Their scheme is simple and easy to implement. However, Tsai et al. shown that their scheme is vulnerable to denial of service attacks, password guessing attack, and privileged insider attack [18]. Recently, Liu et al. proposed an efficient and secure user authentication scheme with a smart card [9]. However, Liu, Tsai, and Hwang shown that their scheme was vulnerable to the replaying attack [8].

Recently, Ramasamy et al. proposed an efficient password authentication scheme for smart cards [14]. However, Thandra et al. showed that their scheme is vulnerable to privileged insider attacks, password guessing attack, and impersonation attack [17]. Thandra et al. also proposed a modified Ramasamy et al.'s scheme to resist the above flaws existing in Ramasamy et al.'s scheme. Thandra et al. claimed that their scheme could resist privileged insider attacks, password guessing attacks, user impersonation attacks, server masquerading attacks, and replay attacks. Furthermore, Thandra et al.'s is able to update user's password and mutual authentication. They used BAN logic to analyze the formal security of their scheme. Their scheme is easy to implement. However, we find their scheme is vulnerable to denial of service attacks, online and offline password guessing attacks, and user impersonation attack.

The rest of this paper is organized as follows. In Section 2, we briefly review Thandra et al.'s password authentication scheme. In Section 3, we analyze and show that some security flaws exist in Thandra et al.' password authentication scheme. Finally, we present our conclusions in Section 4.

TABLE I
The notations used in this paper.

Notations	Meaning
U_i	The user i
ID_i	The identity of the user i
PW_i	The password of the user i
S	The providing service server
(e, n)	The server's public key
D	The server's private key
CID_i	The smart card identity
G	A primitive in both GF_n
$H(\cdot)$	A one-way hash function
T & T_r	The timestamps
$\|\|$	The message concatenation operation

II. Review of Thandra-Rajan-Murty Scheme

In this section, we briefly review Thandra et al.'s password authentication scheme (Thandra-Rajan-Murty Scheme) with smart cards [17]. There are two participants in Thandra-Rajan-Murty's password authentication scheme: a server (S for short) and a user (U for short). The scheme consists of four phases, namely the registration phase, the login phase, the authentication phase, and the password update phase. The notations used in this article are listed in Table I.

A. The Registration Phase

In this phase, the server S makes a smart card for a new user (U_i). The registration phase is executed as follows:

1) The user U_i chooses his/her identity ID_i and password PW_i.
2) U_i computes $h = H(PW_i)$, where $H(\cdot)$ denotes a one-way hash function.
3) U_i sends (ID_i, h) to the server S.
4) S computes CID_i, w_i, and V_i as follows:

$$\begin{aligned} CID_i &= H(ID_i||d), \\ w_i &= CID_i g^h \bmod n, \\ V_i &= g^{CID_i \cdot h \cdot T_r} \bmod n, \end{aligned}$$

where d denotes a private key; (e, n) denotes a public key; $\{d, (e, n)\}$ is a RSA key pair; g denotes a primitive

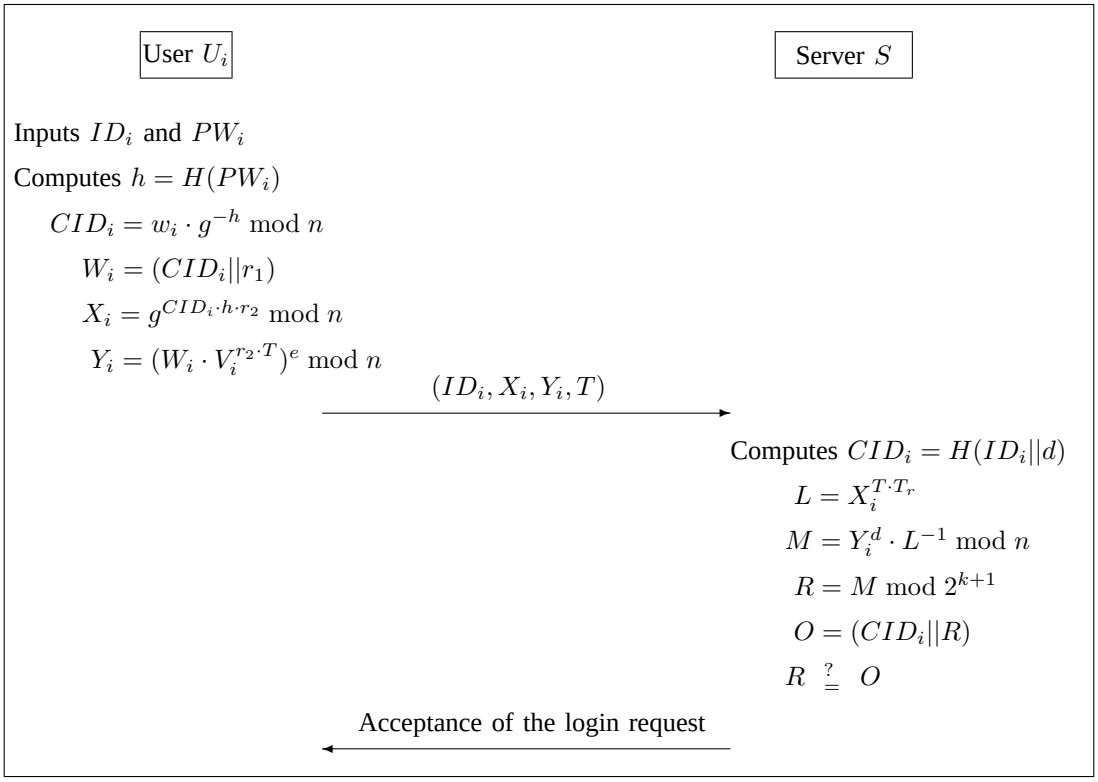

Fig. 1. Login and authentication phases of Thandra-Rajan-Murty scheme

in GF_n; T_r denotes the timestamp of registration of the user.

5) S delivers the smart card to U_i securely. The smart card contains eight parameters, $\{ID_i, w_i, n, e, g, V_i, T_r, H(\cdot)\}$.

B. The Login Phase

In this phase, a user (U_i) wants to login into the server S for obtaining some services, the user first attaches his/her smart card to a device reader and inputs his/her identity ID_i and password PW_i. The login phase is executed in the following and illustrated in Figure 1.

1) The user U_i sends the login request parameters, his/her identity ID_i and password PW_i to the smart card.
2) The smart card computes h and CID_i as follows:

$$\begin{aligned} h &= H(PW_i) \\ CID_i &= w_i g - h \bmod n. \end{aligned}$$

3) The smart card computes W_i, X_i, and Y_i as follows:

$$\begin{aligned} W_i &= (CID_i||r_1); \\ X_i &= g^{CID_i \cdot h \cdot r_2} \bmod n; \\ Y_i &= (W_i V_i r_2 T)^e \bmod n. \end{aligned}$$

Here r_1 and r_2 are two random number selected by the smart card; T denotes the current timestamp of the smart card.

4) The smart card sends (ID_i, X_i, Y_i, T) to the server S.

C. The Authentication Phase

Upon receiving the authentication request message (ID_i, X_i, Y_i, T) from U_i, the server S executes this authentication phase in the following and illustrated in Figure 1.

1) The server S checks whether ID_i format and the timestamp T in valid time or not. If one of conditions does not hold, the server S rejects the login request.
2) S computes CID_i, L, M, R, and O as follows:

$$\begin{aligned} CID_i &= H(ID_i||d); \\ L &= X_i^{T \cdot T_r}; \\ M &= Y_i^d L^{-1} \bmod n; \\ R &= M \bmod (2^{k+1}); \\ O &= (CID_i||R). \end{aligned}$$

3) S compares whether M is equal to O or not. If this condition does not hold, the server rejects the login request.
4) S sends acceptance of the login request to the user if $M = O$.

III. Cryptanalysis of Thandra-Rajan-Murty Scheme

In this section, we will analyze Thandra-Rajan-Murty's password authentication scheme [17]. Thandra et al. claimed that their scheme is resistant to privileged insider attack,

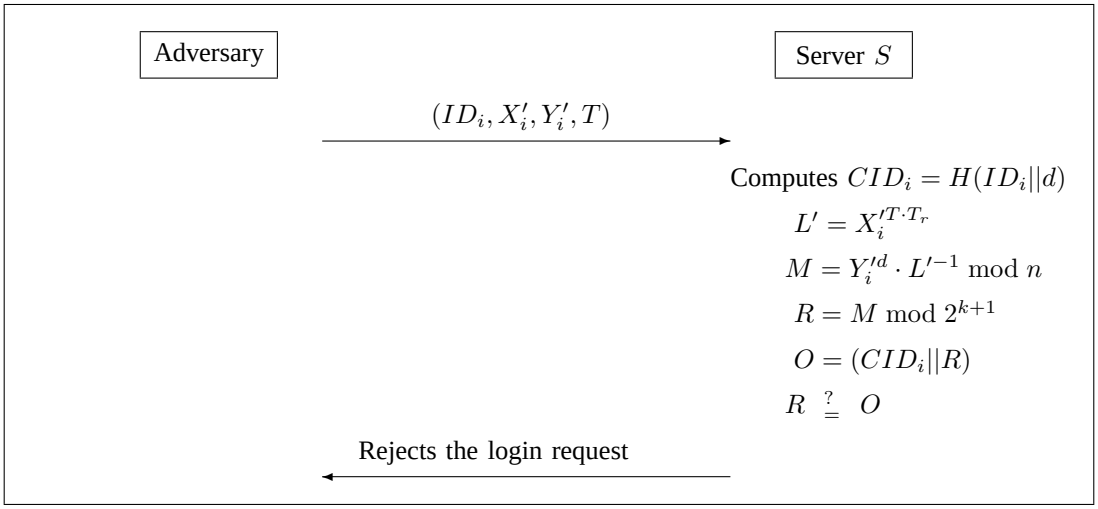

Fig. 2. The denial of service attack on Thandra-Rajan-Murty scheme

password guessing attack, user impersonation attack, server masquerading attack, and replay attack. In this section, we show that Thandra-Rajan-Murty's user password authentication scheme is vulnerable to denial of service attack, online and offline password guessing attack, and impersonation attack.

A. Denial of service attack

In Thandra-Rajan-Murty's scheme, there are two steps needed to be checked for resisting the denial of service attack.

1) The server checks whether the user's identity ID_i and the timestamp T are in correct format and in valid time in Step 1 of the authentication phase.
2) The server checks whether M is equal to O or not in Step 3 of the authentication phase. Here M is computed from Step 2 of the authentication phase.

Next, we show that Thandra-Rajan-Murty's scheme is also vulnerable to the denial of service attack as Figure 2. The adversary may send the modified login request message (ID_i, X_i', Y_i', T') to server, where X_i' and Y_i' are two random numbers; T' is the current timestamp. In this case, the server checks and passes the verification of the user's identity ID_i and the timestamp T in Step 1 of the authentication phase. Thus, the server will continuously execute Step 2 of the authentication phase. Although the server will stop the login request after executing Step 3 of the authentication phase, the server will spend more time to compute CID_i, L, M, R, and O in Step 2 of the authentication phase. Therefore, the denial of service attack might result in the more computation load the server performs.

B. Online Password Guessing Attack

Although, the authors claimed that password guessing is not possible in their scheme [17], because the adversary cannot verify h using any of the known values without knowing the server's secret key. However, we will show that their scheme was vulnerable to the online password guessing attack. The online password guessing attack is executed in the following and illustrated in Figure 3.

Suppose an adversary has stolen the user's smart card. The adversary may guess the user's password PW_i and then observes the communication between the server and the adversary. If the guessing password is correct, the server will send the acceptance of the login request to the user in Step 4 of the authentication phase. Otherwise, the server will terminate this session in Step 3 of the authentication phase. The adversary may guess the other passwords again and repeats to observe the communication between the server and the adversary. Therefore, Thandra-Rajan-Murty's password authentication scheme is vulnerable to the online password guessing attack.

C. Offline Password Guessing Attack

Suppose an adversary has stolen the user's smart card and extracted the parameters $(ID_i, w_i, n, e, g, V_i, T_r)$ from the smart card. The adversary may guess the user's password PW', and then compares V_i whether is equal to $g^{w_i \cdot h_1 \cdot h' \cdot T_r} \bmod n$ or not, where $h_1 = g^{-h'}$ and $h' = H(PW')$. If it is true, the guessing password is correct; otherwise, the password is incorrect. If the adversary has guessed the password PW',

$$\begin{aligned} h' &= H(PW') \\ &= H(PW_i) \\ &= h. \end{aligned}$$

Correctness of the above statement is expressed in the following:

$$\begin{aligned} g^{w_i \cdot h_1 \cdot h' \cdot T_r} \bmod n &= g^{CID_i \cdot g^{h} \cdot g^{-h'} \cdot h' \cdot T_r} \bmod n \\ &= g^{CID_i \cdot h' \cdot T_r} \bmod n \\ &= V_i. \end{aligned}$$

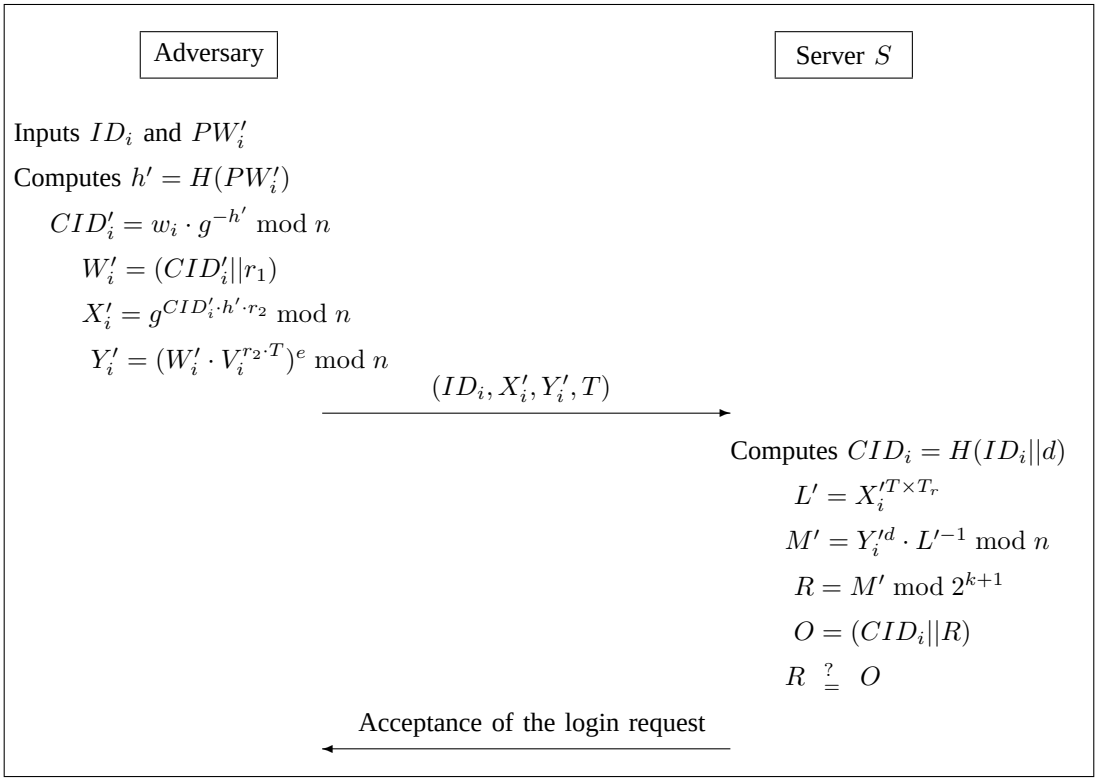

Fig. 3. The online password guessing attack on Thandra-Rajan-Murty scheme

Therefore, Thandra-Rajan-Murty's user password authentication scheme is vulnerable to the offline password guessing attack.

D. Impersonation Attack

Although, the authors claimed that impersonation attack is not possible in their scheme [17], because the decrypted value of Y by the server will not contain proper CID_i for ID_i. However, we will show that their scheme was vulnerable to the impersonation attack. The impersonation attack is executed in the following and illustrated in Figure 4.

Suppose an adversary has stolen the user's smart card and extracted the parameters $(ID_i, w_i, n, e, g, V_i, T_r)$ from the smart card and obtained the password by the offline password guessing attack in Subsection III-C. Then the adversary can impersonate a valid user U_i to login in the server by executing the following steps.

1) The adversary computes X' and Y' as follows:

$$\begin{aligned} X' &= (n-1)^2(T \cdot T_r)^{-1}; \\ CID_i &= w_i \cdot g^{-H(PW_i)}; \\ W &= (CID_i||B); \\ Y' &= W^e(n-1)^2. \end{aligned}$$

   where B is a k-bit number.
2) The adversary could impersonate the user U_i and sends the login request, (ID_i, X', Y', T) to the server.

Upon receiving the authentication request message (ID_i, X', Y', T) from the adversary, the server S executes this authentication phase as follows:

1) The server S checks whether ID_i format and the timestamp T are in valid time or not. ID_i and T are selected by the adversary to meet the correct ID_i and T in valid time.
2) S computes CID_i, L, M, R, and O as follows:

$$\begin{aligned} CID_i &= H(ID_i||d); \\ L &= X'^{T \cdot T_r} \\ &= (n-1)^{-2}(T \cdot T_r)^{-1} \cdot T \cdot T_r \\ &= (n-1)^2; \\ M &= Y'^d \cdot L^{-1} \bmod n \\ &= W^e(n-1)^{2d}(n-1)^{-2} \\ &= W(n-1)^{2(d-1)} \bmod n \\ &= (CID_i||B); \\ R &= M \bmod 2^{k+1} \\ &= B; \\ O &= (CID_i||B). \end{aligned}$$

3) S compares whether M is equal to O or not.
4) S sends the acceptance of the login request to the adversary because of $M = O$.

Therefore, Thandra-Rajan-Murty's user password authentication scheme is vulnerable to the impersonation attack.

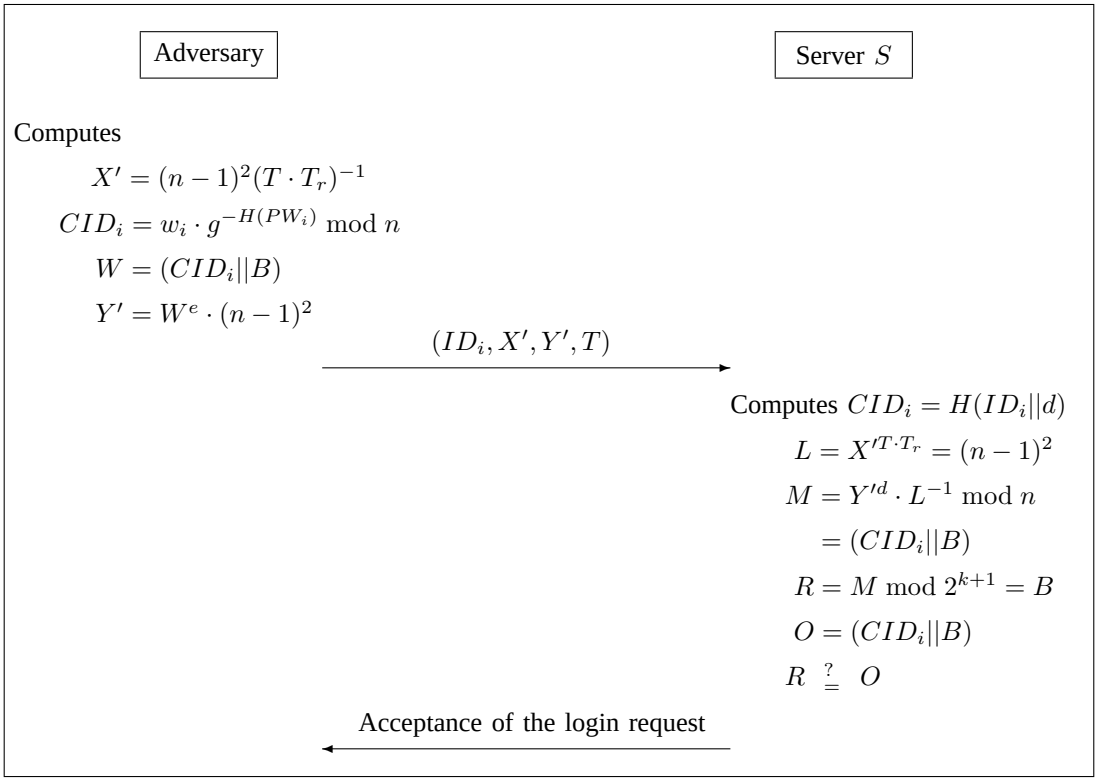

Fig. 4. The impersonation attack on Thandra-Rajan-Murty scheme

IV. Conclusion

In this article, we have reviewed Thandra et al.'s password authentication scheme and cryptanalyzed its security. We showed that Thandra-Rajan-Murty's password authentication scheme [17] cannot withstand the denial of service attack, online and offline password guessing attacks, and impersonation attacks.

Acknowledgment

This study was supported by the National Science Council of Taiwan under grant MOST 104-2221-E-468-004.

References

[1] R. Amin, "Cryptanalysis and Efficient Dynamic ID Based Remote User Authentication Scheme in Multi-server Environment Using Smart Card", *International Journal of Network Security*, Vol. 18, No. 1, pp. 172-181, 2016.

[2] N. Anwar, I. Riadi, A. Luthfi, " Forensic SIM Card Cloning Using Authentication Algorithm", *International Journal of Electronics and Information Engineering*, Vol. 4, No. 2, pp. 71-81, 2016.

[3] C. C. Chang, W. Y. Hsueh, T. F. Cheng, "An Advanced Anonymous and Biometrics-based Multi-server Authentication Scheme Using Smart Cards", *International Journal of Network Security*, Vol. 18, No. 6, pp. 1010-1021, 2016.

[4] M. S. Hwang, L. H. Li, "A New Remote User Authentication Scheme Using Smart Cards", *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 1, pp. 28-30, 2000.

[5] C. C. Lee, M. S. Hwang, I. E. Liao, "Security Enhancement on a New Authentication Scheme with Anonymity For Wireless Environments", *IEEE Transactions on Industrial Electronics*, Vol. 53, No. 5, pp. 1683-1687, 2006.

[6] L. H. Li, I. C. Lin, M. S. Hwang, "A Remote Password Authentication Scheme for Multi-server Architecture Using Neural Networks", *IEEE Transactions on Neural Networks*, Vol. 12, pp. 1498-1504, 2001.

[7] J. Ling, G. Zhao, "An Improved Anonymous Password Authentication Scheme Using Nonce and Bilinear Pairings", *International Journal of Network Security*, Vol. 17, No. 6, pp. 787-794, 2015.

[8] C. W. Liu, C. Y. Tsai, and M. S. Hwang, "Cryptanalysis of an Efficient and Secure Smart Card Based Password Authentication Scheme", *Recent Developments in Intelligent Systems and Interactive Applications*, Lecture Notes in Computer Science, Springer, 2017.

[9] Y. Liu, C. C. Chang, S. C. Chang, "An Efficient and Secure Smart Card Based Password Authentication Scheme", *International Journal of Network Security*, Vol. 19, No. 1, pp. 1-10, 2017.

[10] Y. Liu, C. C. Chang, C. Y. Sun, "Notes on An Anonymous Multi-server Authenticated Key Agreement Scheme Based on Trust Computing Using Smart Card and Biometrics", *International Journal of Network Security*, Vol. 18, No. 5, pp. 997-1000, 2016.

[11] J. W. Lo, J. Z. Lee, M. S. Hwang, Y. P. Chu, "An Advanced Password Authenticated Key Exchange Protocol for Imbalanced Wireless Networks", *Journal of Internet Technology*, Vol. 11, No. 7, pp. 997-1004, 2010.

[12] E. O. Osei, J. B. Hayfron-Acquah, "Cloud Computing Login Authentication Redesign", *International Journal of Electronics and Information Engineering*, Vol. 1, No. 1, pp. 1-8, 2014.

[13] A. Prakash, R. Dhanalakshmi, "Stride Towards Proposing Multi-Modal Biometric Authentication for Online Exam", *International Journal of Network Security*, Vol. 18, No. 4, pp. 678-687, 2016.

[14] R. Ramasamy and A. P. Muniyandi, "An Efficient Password Authentication Scheme for Smart Card", *International Journal of Network Security*, Vol. 14, No. 3, pp. 180-186, 2012.

[15] J. J. Shen, C. W. Lin, M. S. Hwang, "A Modified Remote User Authentication Scheme Using Smart Cards", *IEEE Transactions on Consumer Electronics*, Vol. 49, No. 2, pp. 414-416, 2003.

[16] M. Stanek, "Weaknesses of Password Authentication Scheme Based on Geometric Hashing", *International Journal of Network Security*, Vol. 18, No. 4, pp. 798-801, 2016.

[17] P. K. Thandra, J. Rajan, and S. A. V. S. Murty, "Cryptanalysis of an Efficient Password Authentication Scheme", *International Journal of Network Security*, Vol. 18, No. 2, pp. 362-368, 2016.
[18] C. Y. Tsai, C. S. Pan, and M. S. Hwang, "An Improved Password Authentication Scheme for Smart Card", *Recent Developments in Intelligent Systems and Interactive Applications*, Lecture Notes in Computer Science, Springer, 2017.
[19] Y. Wang and X. Peng, "Cryptanalysis of Two Efficient Password-based Authentication Schemes Using Smart Cards", *International Journal of Network Security*, Vol. 17, No. 6, pp. 728-735, 2015.
[20] J. Wei, W. Liu, X. Hu, "Secure and Efficient Smart Card Based Remote User Password Authentication Scheme", *International Journal of Network Security*, Vol. 18, No. 4, pp. 782-792, 2016.
[21] H. Wijayanto, M. S. Hwang, "Improvement on Timestamp-based User Authentication Scheme with Smart Card Lost Attack Resistance", *International Journal of Network Security*, Vol. 17, No. 2, 2015, pp. 160-164, 2015.
[22] H. Zhu, Y. Zhang, H. Li, and L. Lin, "A Novel Biometrics-based One-Time Commitment Authenticated Key Agreement Scheme with Privacy Protection for Mobile Network", *International Journal of Network Security*, Vol. 18, No. 2, pp. 209-216, 2016.
[23] H. Zhu, Y. Zhang and X. Wang, "A Novel One-Time Identity-Password Authenticated Scheme Based on Biometrics for E-coupon System", *International Journal of Network Security*, Vol. 18, No. 3, pp. 401-409, 2016.
[24] H. Zhu, Y. Zhang, and Y. Zhang, "A Provably Password Authenticated Key Exchange Scheme Based on Chaotic Maps in Different Realm", *International Journal of Network Security*, Vol. 18, No. 4, pp. 688-698, 2016.
[25] X. Zhuang, C. C. Chang, Z. H. Wang, Y. Zhu, "A Simple Password Authentication Scheme Based on Geometric Hashing Function", *International Journal of Network Security*, Vol. 16, pp. 271-277, 2014.