An Improvement of The Remote Authentication Scheme for Anonymous Users Using Elliptic Curves Cryptosystem

Min-Shiang Hwang[1,2], Eko Fajar Cahyadi[1,3], Hung-Wei Yang[1], and Cheng-Ying Yang[4]

[1]Department of Computer Science & Information Engineering
Asia University
Taichung, Taiwan
e-mail: mshwang@asia.edu.tw

[2]Department of Medical Research, China Medical University Hospital
China Medical University
Taichung, Taiwan

[3]Department of Telecommunication Engineering
Institut Teknologi Telkom Purwokerto
Purwokerto, Indonesia
e-mail: ekofajarcahyadi@ittelkom-pwt.ac.id

[4]Department of Computer Science
University of Taipei
Taipei, Taiwan
e-mail: cyang@utaipei.edu.tw

***Abstract*—It is convenient to obtain the information resources via intelligent device over cloud systems. The user authentication mechanism is a fundamental tool for ensuring the validity of communicating party and secure communications among the communicating party. Recently, Zhang, Wang, and Wang proposed a new remote authentication scheme for anonymous users using elliptic curves cryptosystem. Their scheme could achieve the mutual authentication and forward security. They claimed that their scheme could withstand various attacks by employing BAN-logic formal methods. Their claimed that their scheme could withstand the preserving anonymity and non-traceability, perfect forward secrecy, off-line password guessing attack, forgery attack, server impersonating attack, known key attack, and reply attack. However, we will show that their scheme is vulnerable to the forgery attack, server impersonating attack, and man-in-the-middle attack. In this article, we also propose an improved Zhang-Wang-Wang's anonymous user authentication scheme to withstand the vulnerability in their scheme.**

Keywords- mutual authentication; elliptic curves cryptosystem; user authentication; forgery attack, impersonating attack, man-in-the-middle attack.

I. INTRODUCTION

It is convenient to obtain the information resources via intelligent device over cloud systems. The user authentication mechanism is a fundamental tool for ensuring the validity of communicating party and secure communications among the communicating party [1-3]. However, the user authentication mechanisms are vulnerable to various attacks in the public Internet networks. These attacks include password guessing attack, replaying attack, forgery attack, impersonating attack, and man-in-the-middle attack, etc. [4-14]. It's important to design and develop a secure user authentication scheme to resist these attacks.

To authenticate a user from public Internet, many user authentication schemes had been proposed in past decades. Some schemes were applied a smart card to authenticate the legal users [15-26]. Some schemes were developed for multi-servers [27-28]. Some schemes were developed for biometrics [29-32] and some schemes were applied passwords for generating session key [33-34].

Recently, Zhang, Wang, and Wang proposed a new remote authentication scheme for anonymous users using elliptic curves cryptosystem [34]. Their scheme could achieve the mutual authentication and forward security. They claimed that their scheme could withstand various attacks by employing BAN-logic formal methods. Their claimed that their scheme could withstand the preserving anonymity and non-traceability, perfect forward secrecy, off-line password guessing attack, forgery attack, server impersonating attack, known key attack, and reply attack. However, we will show that their scheme is vulnerable to the forgery attack, server impersonating attack, and man-in-the-middle attack. In this article, we also propose an improved Zhang-Wang-Wang's anonymous user authentication scheme to withstand the vulnerability in their scheme.

The rest of this article is organized as follows. In Section 2, we review Zhang-Wang-Wang's remote authentication scheme for anonymous users using elliptic curves cryptosystem briefly. In Section 3, we show that Zhang-Wang-Wang's scheme suffers from the forgery and server impersonating, man-in-the middle attacks. In Section 4, we propose an improvement of Zhang-Wang-Wang's scheme and security analysis of the improved scheme. Finally, some conclusions are summarized in Section 5.

II. REVIEW OF ZHANG-WANG-WANG'S SCHEME

There are two main participants in Zhang-Wang-Wang's scheme: a user U_i and server S [34]. There are four phases in Zhang-Wang-Wang's scheme: The registration phase, the login phase, the authentication and session key exchange phase, and the password updating phase. We briefly describe Zhang-Wang-Wang's scheme as follows.

A. *The Registration Phase*

In this registration phase, a new user (U_i) needs to apply to the server for as a legal user. After the phase, the server will make and issue a smart card for the new user (U_i). The smart card contains the following seven parameters: {r, B_i, p, $E_p()$, P, Q, H()}, here r is a random number choice by the new user; H() is a one-way hash function; $E_p()$ is an elliptic curve in the finite field Z_p. B_i and Q computed as follows:

$B_i = X_i \oplus H(ID_i \parallel A_i)$

$X_i = H(x\ ID_i\ Q)$

$Q = xP \bmod p$

$A_i = H(r \parallel PW_i)$.

Where x is a master secret key of the server S; p is a large prime number.

B. *The Login Phase*

In this phase, when the user (U_i) wants to have the access right to obtain the resources provided by the remote server, U_i keys in his/her identity (ID_i) and password (PW_i) to the terminal devise with smart card. The smart card sends the login message {C_i, R_i, V_i, T_i} to the server S. Here T_i is a fresh current timestamp. C_i, R_i and V_i are computed as follows:

$C_i = ID_iP + aQ$

$R_i = aP$

$V_i = X_i \oplus H(aQ \parallel T_i)$

$X_i = B_i \oplus H(ID_i \parallel A_i)$

$A_i = H(r \parallel PW_i)$.

Where *a* is a random nonce which is generated by the smart card.

C. *The Authentication and Session Key Exchange phase*

Once the server receives the login request message {C_i, R_i, V_i, T_i} from the smart card, the user (U_i) and the server S mutual verify in this authentication phase as follows.

1) The server S verifies the validity of the time stamp T_i. If T_i is not in the current interval time, the server rejects the login request.
2) The server calculates $V_i^* = H(x^2 (C_i – xR_i)) \oplus H(xR_i \parallel T_i)$. S checks whether V_i^* is equal to V_i. If it is not hold, the server rejects the login request.
3) The server S replies the message {R_s, V_s, T_s} to the user U_i, here T_s is the current time stamp of the server. Rs and Vs are computed as follows:

   $R_s = bP$;

   $V_s = H(ID_i\ P \parallel bR_i \parallel T_s)$;

   Here b is a random number which is generated by the server.
4) Upon receiving {R_s, V_s, T_s} from the server, the user U_i verifies the validity of the time stamp T_s. If T_s is in the current interval time, the user calculates $V_s^* = H(ID_i\ P \parallel aR_s \parallel T_s)$ and checks whether V_s^* is equal to V_s. If it holds, the user authenticates the legality of the server. Otherwise, the user terminates the session connection.
5) The server computes the session key: $SK = bR_i{=}baP$. The user computes the session key: $SK = aR_s = abP$.

D. *Password Updating Phase*

In this phase, the user (U_i) wants to update his/her current password (PW_i) to a new one ($PW`_i$). The smart card executes the following procedures:

1) The smart card asks the user inputs his/her ID_i and PW_i.
2) The smart card calculates the new $B`_i$ as follows:

   $A_i = H(r \parallel PW_i)$

   $A`_i = H(r \parallel PW`_i)$

   $B`_i = B_i \oplus H(ID_i \parallel A_i) \oplus H(ID_i \parallel A'_i)$

   $= X_i \oplus H(ID_i \parallel A_i) \oplus H(ID_i \parallel A_i) \oplus H(ID_i \parallel A`_i)$

   $= X_i \oplus H(ID_i \mid A`_i)$
3) The smart card replaces the original B_i with the new $B`_i$.

III. The Weakness of Zhang-Wang-Wang Scheme

In this section, we show the weakness of Zhang-Wang-Wang's smart card-based authentication scheme [34]. The main weakness of Zhang-Wang-Wang's scheme is that their scheme could not withstand the on-line password guessing attack with user's smart card and the denial of service attack.

A. *The Forgery Attack*

In this subsection, we will show that an adversary could masquerade as other legitimate users in Zhang-Wang-Wang scheme.

1).The adversary intercepted the login request message {C_i, R_i, V_i, T_i} between the legal user U_i and the server in the login phase.

2) The adversary sends the login message {C_c, R_c, V_c, T_c} to the server S. Here T_c is a fresh current timestamp. $V`_i$ is computed as follows:

   $aQ = C_i - ID_iP$

   $X_i = V_i \oplus H(aQ \parallel T_i)$

   $C_c = ID_iP + cQ$

   $R_c = cP$

   $V_c = X_i \oplus H(cQ \parallel T_c)$.

   Here, c is a random nonce which is generated by the adversary.

3) The server S verifies the validity of the time stamp T_c. If T_c is not in the current interval time, the server rejects the login request. Since the T_c is the fresh time stamp, the server will accept it in this step.

4) The server calculates $V_i^* = H(x^2 (C_c - xR_c)) \oplus H(xR_c \parallel T_c)$. S checks whether V_i^* is equal to V_c. If it is not hold, the server rejects the login request. In this step, we will show that V_i^* is equal to V_c as follows:

   $V_i^* = H(x^2 (C_c - xR_c)) \oplus H(xR_c \parallel T_c)$.

   $= H(x^2 (ID_iP + cQ - xR_c)) \oplus H(xR_c \parallel T_c)$.

   $= H(x^2 (ID_iP + cxP - xcP)) \oplus H(xcP \parallel T_c)$.

   $= H(x\ x\ ID_i\ P) \oplus H(cQ \parallel T_c)$.

   $= H(x\ ID_i\ Q) \oplus H(cQ \parallel T_c)$.

   $= X_i \oplus H(cQ \parallel T_c)$.

   $= V_c$

5) The server S replies the message {R_s, V_s, T_s} to the adversary, here T_s is the current time stamp of the server. R_s and V_s are computed as follows:

$R_s = bP$;

$V_s = H(ID_i\ P \| bR_c \| T_s)$;

Here b is a random number which is generated by the server.

6) Upon receiving $\{R_s, V_s, T_s\}$ from the server, the adversary verifies the validity of the time stamp T_s. If T_s is in the current interval time, the adversary calculates $V_s^* = H(ID_i\ P \| aR_s \| T_s)$ and checks whether V_s^* is equal to V_s. If it holds, the user authenticates the legality of the server. Otherwise, the user terminates the session connection.
7) The server computes the session key: $SK = bR_c{=}bcP$. The adversary computes the session key: $SK = cR_s = cbP$.

In the above steps, the server will mistake the adversary as the legal user U_i. The adversary will masquerade as the user U_i to have a secure communication with the server with the common session key SK.

B. The Server Impersonating Attack

In this subsection, we will show that an adversary could masquerade as the legitimate server in Zhang-Wang-Wang scheme.

1). The user (U_i) keys in his/her identity (ID_i) and password (PW_i) to the terminal devise with smart card. The smart card sends the login message $\{C_i, R_i, V_i, T_i\}$ to the server S. Here C_i, R_i, V_i, and T_i are the same as those in the login phase of Zhang-Wang-Wang's scheme.

2) The adversary masquerades the server to reply the message $\{R`_s, V`_s, T_s\}$ to the user U_i, here T_s is the current time stamp of the adversary. $R`_s$ and $V`_s$ are computed as follows:

$R`_s = cP$;

$V`_s = H(ID_i\ P \| cR_i \| T_s)$;

Here c is a random number which is generated by the adversary.

3) Upon receiving $\{R`_s, V`_s, T_s\}$ from the adversary, the user verifies the validity of the time stamp T_s. If T_s is in the current interval time, the user calculates $V_s^* = H(ID_i\ P \| aR`_s \| T_s)$ and checks whether $V_s^*$ is equal to $V`_s$. If it holds, the user authenticates the legality of the server. Otherwise, the user terminates the session connection. In this step, we will show that V_s^* is equal to $V`_s$ as follows:

$V_s^* = H(ID_i\ P \| aR`_s \| T_s)$

$= H(ID_i\ P \| acP \| T_s)$

$= H(ID_i\ P \| caP \| T_s)$

$= H(ID_i\ P \| cR_i \| T_s)$

$= V`_s$

4) The user computes the session key: $SK = aR`_s = acP$. The adversary computes the session key: $SK = cR_i = caP$.

In the above steps, the user will mistake the adversary as the legal server. The adversary will masquerade as the server to have a secure communication with the user with the common session key SK.

C. The Man-in-the-Middle Attack

In this subsection, we will show that an adversary could hide in the middle to eavesdrop the secret message between the legal user and the server in Zhang-Wang-Wang scheme.

1). The user (U_i) keys in his/her identity (ID_i) and password (PW_i) to the terminal devise with smart card. The smart card sends the login message $\{C_i, R_i, V_i, T_i\}$ to the server S. Here T_i is a fresh current timestamp. C_i, R_i and V_i are computed as follows:

$C_i = ID_iP + aQ$

$R_i = aP$

$V_i = X_i \oplus H(aQ \| T_i)$

$X_i = B_i \oplus H(ID_i \| A_i)$

$A_i = H(r \| PW_i)$.

Where *a* is a random nonce which is generated by the smart card.

2) The adversary intercepted the login request message $\{C_i, R_i, V_i, T_i\}$ between the legal user U_i and the server in the login phase. The adversary sends the login message $\{C_c, R_c, V_c, T_c\}$ to the server S. Here T_c is a fresh current timestamp. $V`_i$ is computed as follows:

$aQ = C_i - ID_iP$

$X_i = V_i \oplus H(aQ \| T_i)$

$C_c = ID_iP + cQ$

$R_c = cP$

$V_c = X_i \oplus H(cQ \| T_c)$.

Here, c is a random nonce which is generated by the adversary.

3) The server S verifies the validity of the time stamp T_c. If T_c is not in the current interval time, the server rejects the login request.
4) The server calculates $V_i^* = H(x^2\ (C_c - xR_c)) \oplus H(xR_c \| T_c)$. S checks whether V_i^* is equal to V_c. If it is not hold, the server rejects the login request.
5) The server S replies the message $\{R_s, V_s, T_s\}$ to the adversary, here T_s is the current time stamp of the server. R_s and V_s are computed as follows:

$R_s = bP$;

$V_s = H(IDi\ P \| bR_c \| T_s)$;

Here b is a random number which is generated by the server.

6) Upon receiving $\{R`_s, V`_s, T_s\}$ from the server, the adversary replies the message $\{R`_s, V`_s, T_s\}$ to the user U_i. $R`_s$ and V`s are computed as follows:

$R`_s = cP$;

$V`_s = H(ID_i\ P \| cR_i \| T_s)$;

7) Upon receiving $\{R`_s, V`_s, T_s\}$ from the adversary, the user Ui verifies the validity of the time stamp Ts. If T_s is in the current interval time, the user calculates $V_s^* = H(ID_i\ P \| aR`_s \| T_s)$ and checks whether $V_s^*$ is equal to $V`_s$. If it holds, the user authenticates the legality of the server. Otherwise, the user terminates the session connection.
8) The server computes the session key: $SK_{sa} = bR_c{=}bcP$. The user computes the session key: $SK_{ia} = aR`_s{=}acP$. The adversary computes two session keys:

$SK_{as} = cR_s = cbP=bcP=SK_{sa}$.

$SK_{ai} = cR_i = caP = acP = SK_{ia}$.

IV. The Improved Zhang-Wang-Wang Scheme

In order to improve the weakness of Zhang-Wang-Wang's remote authentication scheme for anonymous users using elliptic curves cryptosystem, we propose an improvement of Zhang-Wang-Wang's scheme in this section. The password updating phase is the same as that in Zhang-Wang-Wang's scheme.

A. The Registration Phase

In this registration phase, a new user (U_i) needs to apply to the server for as a legal user. After the phase, the server will make and issue a smart card for the new user (U_i). The smart card contains the following eight parameters: {r, A_i, B_i, p, $E_p()$, P, Q, H()}, here r, H(), and $E_p()$ are the same as that in Zhang-Wang-Wang's scheme. A_i, B_i, p and Q computed as follows:

$A_i = H(r \| ID_i \| PW_i)$

$Q = xP \bmod p$

$X_i = H(x\ ID_i\ A_i\ Q)$

$B_i = X_i \oplus H(ID_i \| A_i)$

Where x is a master secret key of the server S.

B. The Login Phase

In this phase, when the user (U_i) wants to have the access right to obtain the resources provided by the remote server, U_i keys in his/her identity (ID_i*) and password (PW_i*) to the terminal devise with smart card.

1) The smart card computes A_i* as follows:

$A_i^* = H(r \| ID_i^* \| PW_i^*)$.

The smart card checks whether A_i* is equal to A_i which stored in the smart card. If it holds, the smart card continually executes the following step. Otherwise, the smart card asks the user re-inputs his/her identity (ID_i*) and password (PW_i*). If the user fails to input ID_i and PW_i for three times, the smart card stops the login request.

2) The smart card sends the login message {C_i, R_i, V_i, T_i} to the server S. Here R_i, V_i, and T_i are the same as that in the login phase of Zhang-Wang-Wang's scheme. Ci is computed as follows:

$C_i = ID_i\ A_i\ P + aQ$

Where *a* is a random nonce which is generated by the smart card.

C. The Authentication and Session Key Exchange phase

Once the server receives the login request message {C_i, R_i, V_i, T_i} from the smart card, the user (U_i) and the server S mutual verify in this authentication phase as follows.

1) The server S verifies the validity of the time stamp T_i. If T_i is not in the current interval time, the server rejects the login request.

2) The server calculates X_i* and $V_i^* = X_i^* \oplus H(xR_i \| T_i)$. S checks whether V_i* is equal to V_i. If it is not hold, the server rejects the login request. We show that the legal user will make V_i* = V_i as follows:

$X_i^* = H(x^2 (C_i - xR_i))$

$= H(x^2 (ID_i\ A_i\ P + aQ - xR_i))$

$= H(x^2 (ID_i\ A_i\ P + axP - xaP))$

$= H(x\ A_i\ x\ ID_i\ P)$

$= H(x\ ID_i\ A_i\ Q)$

$= X_i$

$V_i^* = X_i^* \oplus H(xR_i \| T_i)$.

$= X_i^* \oplus H(xaP \| T_i)$.

$= X_i^* \oplus H(aQ \| T_i)$.

$= V_i$

3) The server S replies the message {R_s, V_s, T_s} to the user U_i, here T_s is the current time stamp of the server. R_s and V_s are computed as follows:

$R_s = bP$;

$V_s = H(ID_i\ P \| bR_i \| X_i \| T_s)$;

Here b is a random number which is generated by the server.

4) Upon receiving {R_s, V_s, T_s} from the server, the user U_i verifies the validity of the time stamp T_s. If T_s is in the current interval time, the user calculates $V_s^* = H(ID_i\ P \| aR_s \| X_i \| T_s)$ and checks whether V_s* is equal to V_s. If it holds, the user authenticates the legality of the server. Otherwise, the user terminates the session connection. Here X_i is retrieved from the smart card.

5) The server computes the session key: $SK = bR_i=baP$. The user computes the session key: $SK = aR_s = abP$.

D. Security Analysis of The Improved Scheme

In this subsection, we will present that the improved scheme has the ability to against the forgery attack, server impersonating attack, and man-in-the-middle attack.

1).To against the forgery attack: The main vulnerability in this attack of Zhang-Wang-Wang's scheme is that an adversary could intercept the login request message {C_i, R_i, V_i, T_i} between the legal user U_i and the server in the login phase. The adversary could derive aQ with public information ID_i and P (see Section IIIA). In the improved scheme, $C_i = ID_i\ A_i\ P + aQ$. The adversary is unable to derive aQ with knowing C_i, ID_i, and P and un-known A_i. Therefore, the improved scheme has the ability to against the forgery attack.

2).To against the server impersonating attack: The main vulnerability in this attack of Zhang-Wang-Wang's scheme is that an adversary could fabricate {$R`_s$, V` The adversary masquerades the server to reply the message {$R`_s$, $V`_s$, T_s} to the user U_i. Here, T_s is the current time stamp of the adversary. The adversary generates a random number c and knows ID_i, P, and R_i, thus $R`_s$ and $V`_s$ are computed (see Section IIIB). In the improved scheme,

$V_s = H(ID_i\ P \| bRi \| X_i \| T_s)$.

The adversary doesn't know the secret X_i. Therefore, he/she is unable to fabricate V_s and thus the improved scheme has the ability to against the server impersonating attack.

3).To against the man-in-the middle attack: The main vulnerability in this attack of Zhang-Wang-Wang's scheme is that their scheme could not against the forgery attack and the server impersonating attack. We have shown that the improved scheme has the ability to against the forgery attack and the server impersonating attack. Therefore, the improved scheme also could against the man-in-the-middle attack.

V. Conclusions

In summary, we have shown that the weakness of Zhang-Wang-Wang's remote authentication scheme for anonymous users using ECC. Zhang-Wang-Wang’s scheme could not withstand the forgery attack, server impersonating attack, and man-in-the-middle attack. In this article, we also proposed an improvement of Zhang-Wang-Wang’s anonymous user authentication scheme to withstand the vulnerability in their scheme.

Acknowledgment

This work was partially supported by the Ministry of Science and Technology, Taiwan, R.O.C., under contract no.: MOST 106-3114-E-005-001, MOST 106-2221-E-468-002, and MOST 106-2221-E-845-001.

References

[1] Tsai, C.S., Lee, C.C., Hwang, M.S.: Password authentication schemes: current status and key issues. International Journal of Network Security 3, 101-115 (2006).

[2] Zhuang, X., Chang, C.C., Wang, Z.H., Zhu, Y.: A simple password authentication scheme based on geometric hashing function. International Journal of Network Security 16, 271-277 (2014).

[3] Zhu, H., Zhang, Y.: An improved two-party password-authenticated key agreement protocol with privacy protection based on chaotic maps. International Journal of Network Security 19(4), 487-497 (2017).

[4] Yang, C.C., Chang, T.Y., Hwang, M.S.: The security of the improvement on the methods for protecting password transmission. Informatica 14, 551-558 (2003).

[5] Ling, C.H., Chao, W.Y., Chen, S.M., Hwang, M.S.: Cryptanalysis of dynamic identity based on a remote user authentication scheme for a multi-server environment. In: Advances in Engineering Research Vol. 15, pp. 981-986. Atlantis Press (2015).

[6] Pan, H.T., Pan, C.S., Tsaur, S.C., Hwang, M.S.: Cryptanalysis of efficient dynamic ID based remote user authentication scheme in multi-server environment using smart card. In: 12th International Conference on Computational Intelligence and Security, Wuxi, China, pp. 590-593 (2017).

[7] He, D., Chen, J., Hu, J.: Weaknesses of a remote user password authentication scheme using smart card. International Journal of Network Security 13, 58-60 (2011).

[8] Feng, T.H., Chao, W.Y., Hwang, M.S.: Cryptanalysis and improvement of the Li-Liu-Wu user authentication scheme. In: International Conference on Future Communication Technology and Engineering, pp. 103-106, Shenzhen China (2014).

[9] Chen, T.Y., Ling, C.H., Hwang, M.S.: Weaknesses of the Yoon-Kim-Yoo remote user authentication scheme using smart cards. In: IEEE Workshop on Electronics, Computer and Applications, Ottawa, Canada, pp. 771-774 (2014).

[10] Amin, R.: Cryptanalysis and efficient dynamic ID based remote user authentication scheme in multi-server environment using smart card. International Journal of Network Security 18(1), 172-181 (2016).

[11] Mohan, N.B.M., Chakravarthy, A.S.N., Ravindranath, C.: Cryptanalysis of design and analysis of a provably secure multi-server authentication scheme. International Journal of Network Security 20(2), 217-224 (2018).

[12] Feng, T.H., Ling, C.H., Hwang, M.S.: Cryptanalysis of Tan's improvement on a password authentication scheme for multi-server environments. International Journal of Network Security 16, 318-321 (2014).

[13] He, D., Zhao, W., Wu, S.: Security analysis of a dynamic id-based authentication scheme for multi-server environment using smart cards. International Journal of Network Security15, 282-292 (2013).

[14] Li, J., Liu, S., Wu, S.: Cryptanalysis and improvement of a YS-like user authentication scheme. International Journal of Digital Content Technology and its Applications 7(1), 828-836 (2012).

[15] Liu, Y., Chang, C.C., Chang, S.C.: An efficient and secure smart card based password authentication scheme. International Journal of Network Security 19(1), 1-10 (2017).

[16] Shen, J.J., Lin, C.W., Hwang, M.S.: Security enhancement for the timestamp-based password authentication scheme using smart cards. Computers & Security 22, 591-595 (2003).

[17] Shen, J.J., Lin, C.W., Hwang, M.S.: A modified remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics 49, 414-416 (2003).

[18] Tang, H., Liu, X., Jiang, L.: A robust and efficient timestamp-based remote user authentication scheme with smart card lost attack resistance. International Journal of Network Security 15, 446-454 (2013).

[19] Yang, L., Ma, J.F., Jiang, Q.: Mutual authentication scheme with smart cards and password under trusted computing. International Journal of Network Security 14, 156-163 (2012).

[20] Ghosh, D., Li, C., Yang, C.: A lightweight authentication protocol in smart grid. International Journal of Network Security 20(3), 414-422 (2018).

[21] Li, C.T., Hwang, M.S.: An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards. International Journal of Innovative Computing, Information and Control 6, 2181-2188 (2010).

[22] Li, C.T., Hwang, M.S.: An efficient biometrics-based remote user authentication scheme using smart cards. Journal of Network and Computer Applications 33, 1-5 (2010).

[23] Yoon, E.J., Kim, S.H., Yoo, K.Y.: A security enhanced remote user authentication scheme using smart cards. International Journal of Innovative Computing, Information and Control 8(5), 3661-3675 (2012).

[24] Huang, H.F., Chang, H.W., Yu, P.K: Enhancement of timestamp-based user authentication scheme with smart card. International Journal of Network Security 16, 463-467 (2014).

[25] Feng, T.H., Ling, C.H., Hwang, M.S.: An improved timestamp-based user authentication scheme with smart card. In: The 2nd Congress on Computer Science and Application, pp. 111-117, Sanya, China (2014).

[26] Chang, C. C., Lee, C. Y.: A smart card-based authentication scheme using user identity cryptography. International Journal of Network Security 16, 139-147 (2013).

[27] Li, L.H., Lin, I.C., Hwang, M.S.: A remote password authentication scheme for multi-server architecture using neural networks. IEEE Transactions on Neural Networks 12, 1498-1504 (2001).

[28] Lin, I.C., Hwang, M.S., Li, L.H.: A new remote user authentication scheme for multi-server architecture. Future Generation Computer Systems 19, 13-22 (2003).

[29] Prakash, A.: A biometric approach for continuous user authentication by fusing hard and soft traits. International Journal of Network Security 16, 65-70 (2014).

[30] Li C.T. Hwang, M.S.: An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards. *International Journal of Innovative Computing, Information and Control* 6 (2010) 2181-2188.

[31] C. T. Li, M. S. Hwang. 2010. An Efficient Biometrics-Based Remote User Authentication Scheme Using Smart Cards. *Journal of Network and Computer Applications* 33 (2010) 1-5.

[32] A. Prakash. 2014. A Biometric Approach For Continuous User Authentication By Fusing Hard And Soft Traits. International Journal of Network Security 16 (2014) 65-70.

[33] Wu, M., Chen, J., Wang, R.: An enhanced anonymous password-based authenticated key agreement scheme with formal proof. International Journal of Network Security 19(5), 785-793 (2017).

[34] Xueqin Zhang, Baoping Wang, and Wei Wang: A New Remote Authentication Scheme for Anonymous Users Using Elliptic Curves Cryptosystem. International Journal of Network Security 20(2), 390-395 (2018).