

# Cryptanalysis of and Improvement on Biometric-based User Authentication Scheme for C/S System

Yoonsung Choi, Dongho Won

**Abstract**— Password-based authentication schemes are convenient, but vulnerable to simple dictionary attacks. Cryptographic secret keys are safe, but difficult to memorize. More recently, biometric information has been used for authentication schemes. Das proposed a biometric-based authentication scheme, but it has various vulnerabilities. Jiping et al. improved Das's scheme, but some vulnerabilities remain. In this paper, we analyze the cryptanalysis of Jiping et al.'s authentication scheme and propose the security enhanced biometric-based user authentication scheme for the C/S System.

## I. INTRODUCTION

Remote identity-based authentication schemes are based on using only passwords. The password-based authentication schemes are the simple and convenient method to have a user authenticated in order to provide services of a computing or communication system [1-7]. However, only passwords are easy to break by using simple dictionary attacks. To overcome this problem, cryptographic secret keys and passwords are used in the remote user authentication schemes [8-10]. But the long and random cryptographic keys are difficult to memorize. So they must be stored somewhere, it is very weak point. To solve problem, various biometric-based authentication schemes are proposed. Das proposed new authentication scheme but has various vulnerability [11], so Jiping et al proposed the security improved biometric-based user authentication scheme for C/S system than Das's scheme [12]. But Jiping et al's scheme still has security problems. In section 2, we study related works. In section 3, we briefly review the Jiping et al's biometric-based remote user authentication scheme using smart cards. In section 4, we analyze the security vulnerability of Jiping et al's authentication scheme and suggest solution. Finally, we conclude the paper in section 5.

## II. RELATED WORKS

### A. Smart card Attack

Various researchers have observed that confidential information stored in all smart cards could be extracted by physically monitoring power consumption like SPA and DPA. When a user loses a smart card, an attacker can analyze it. So various schemes leave it vulnerable to off-line password attacks. And attacker can be authenticate to server without user's ID and password.

### B. Biometric-based Authentication

Biometrics refers to the quantifiable data related to human characteristics and traits. Example include to fingerprint, face recognition, DNA, palm print, hand geometry, iris, retina, odour/scent, typing rhythm, gait, and voice. Biometrics-based authentication is used in identification and access control. Biometric information cannot be lost or forgotten and is very difficult to copy or share and forge or distribute. And also, biometric information cannot be guessed easily and is not easier to break than others.

### C. Das's Biometric-based User Authentication Scheme

Das proposed biometric-based remote user authentication which is inherently more reliable and secure than usual traditional password-based remote authentication schemes. But this scheme has security vulnerability to replay attack, denial-of-service attack, user impersonation attack, and password change problem. Moreover, this scheme does not provide mutual authentication between the user and server.

## III. REVIEW OF JIPING ET AL.'S SCHEME

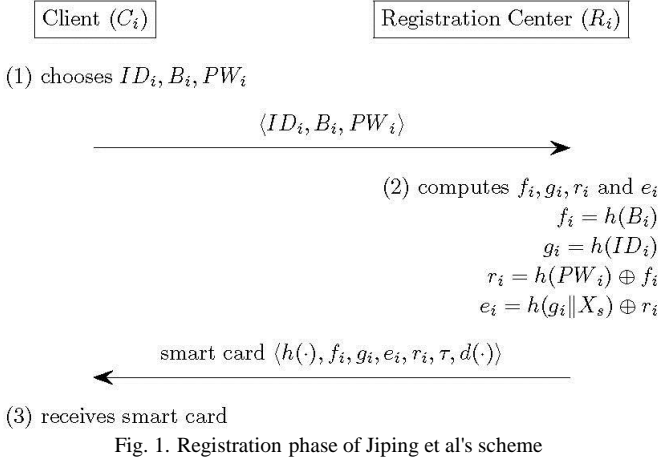
Das proposes biometric-based authentication scheme but this scheme is various security problems. To solve these problems, Jiping et al proposed improved biometric-based authentication scheme [12]. For convenience, we use notations shown in Table 1.

TABLE I: NOTATION

Notation	Description
$C_i$	Client
$S_i$	Server
$R_i$	Registration center
$PW_i$	Password shared between $C_i$ and $S_i$
$ID_i$	Identity of the user $C_i$
$B_i$	Biometric template of the user $C_i$
$d(\cdot)$	Symmetric parametric function
$\tau$	Predetermined threshold
$h(\cdot)$	A secure one-way hash function
$X_s$	A secret information maintained by the server
$R_c$	A random number chosen by $C_i$
$R_s$	A random number chosen by $S_i$
$A \parallel B$	Data $A$ concatenates with data $B$
$A \oplus B$	XOR operation of $A$ and $B$

### A. Registration Phase

In the registration phase, remote user  $C_i$  has to perform the following registration steps. Figure 1 shows the registration phase of Das scheme.



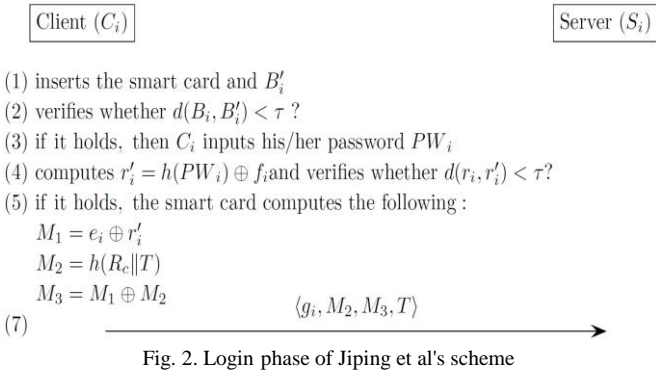
(1) The user  $C_i$  inputs personal biometric  $B_i$  on a device and sends the identity  $ID_i$  and password  $PW_i$  to the registration center  $R_i$  in person.

(2) The registration center  $R_i$  computes  $f_i = h(B_i)$ ,  $g_i = h(ID_i)$ ,  $r_i = h(PW_i) \oplus f_i$ , and  $e_i = h(g_i \| X_s) \oplus r_i$ .  $X_s$  is secret information shared by  $R_i$  and  $S_i$ .  $X_s$  and passwords of the corresponding users are not disclosed to any others for all secure future communications.

(3) Registration center  $R_i$  loads  $(h(\cdot), f_i, g_i, e_i, r_i, \tau, d(\cdot))$  on the user's smart card and sends this information to the user  $C_i$  using a secure channel.

### B. Login Phase

In the login phase, remote user  $C_i$  has to perform the following login steps. Figure 2 show the login phase.



(1)  $C_i$  first inserts user's smart card into the card reader of a terminal and inputs user's biometric template,  $B'_i$ , on the device. If  $d(B_i, B'_i) > \tau$ , login phase is terminated. Otherwise,  $C_i$  passes the biometric verification and then inputs user's password  $PW_i$ .

(2) Smart card computes  $r'_i = h(PW_i) \oplus f_i$ . If  $d(r'_i, r_i) > \tau$ , then password is not correct, so the system terminates the session; otherwise, the smart card computes  $M_1 = e_i \oplus r'_i$ , which is equal to  $h(g_i \| X_s)$ ,  $M_2 = h(R_c \| T)$ , where  $R_c$  is a random number generated by the user  $C_i$  and  $T$  is the current timestamp of  $C_i$ 's system, and  $M_3 = M_1 \oplus M_2$ .

(3) Finally, the user  $C_i$  sends the message  $\langle g_i, M_2, M_3, T \rangle$  to the remote server  $S_i$ .

### C. Authentication Phase

In the authentication phase, remote user  $C_i$  and server  $S_i$  have to perform the following authentication phase. When the remote server  $S_i$  receives the login message  $\langle g_i, M_2, M_3, T \rangle$  at time  $T^*$ , it will perform the following steps as shown in figure 3 to authenticate whether the user  $C_i$  is legitimate or not. Figure 3 show the authentication phase.

(1) Check T. If  $(T^* - T) > \Delta T$ , the authentication phase is terminated, where  $\Delta T$  is the expected time interval for the transmission delay of the system. Otherwise, if  $(T^* - T) \leq \Delta T$ , the authentication steps will be performed.

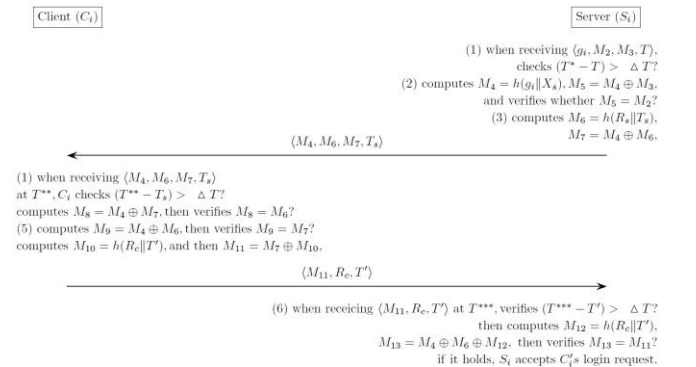
(2).  $S_i$  checks the accuracy of  $C_i$ 's  $ID_i$ . It computes  $M_4 = h(g_i \| X_s)$  using the secret value  $X_s$  maintained by the server  $S_i$  and then computes  $M_5 = M_4 \oplus M_3$  and verifies whether  $M_5 = M_2$  or not. If it does not accurate, then  $S_i$  rejects  $C_i$ 's login request. The verification is successful, the next step will be performed.

(3)  $S_i$  computes  $M_6 = h(R_s \| T_s)$  and  $M_7 = M_4 \oplus M_6$ , where  $T_s$  is the timestamp of the server  $S_i$ , and then  $S_i$  sends message  $\langle M_4, M_6, M_7, T_s \rangle$  to the user  $C_i$ .

(4) After receiving the message  $\langle M_4, M_6, M_7, T_s \rangle$  at time  $T^{**}$ ,  $C_i$  checks the freshness of  $T_s$  by verifying  $(T^{**} - T_s) > \Delta T$ . If it holds, the following session is terminated; otherwise  $C_i$  computes  $M_8 = M_4 \oplus M_7$  and then verifies whether  $M_8 = M_6$ . If it does not hold,  $C_i$  terminates the session. Otherwise, it goes to the next step.

(5)  $C_i$  computes  $M_9 = M_4 \oplus M_6$  and then verifies whether  $M_9 = M_7$ . If it does not hold,  $S_i$  is rejected by  $C_i$ ; otherwise, if it holds,  $C_i$  computes  $M_{10} = h(R_c \| T')$ , where  $T'$  is the current timestamp of the user  $C_i$ , and then computes  $M_{11} = M_7 \oplus M_{10}$  and sends the message  $\langle M_{11}, R_c, T' \rangle$  to the remote server  $S_i$ .

Step 6. When  $S_i$  receives the message  $\langle M_{11}, R_c, T' \rangle$  at time  $T^{***}$ , it checks  $(T^{***} - T') > \Delta T$ . If it holds, the authentication phase is terminated. Otherwise, if it does not hold,  $S_i$  computes  $M_{12} = h(R_c \| T')$  and then computes  $M_{13} = M_4 \oplus M_6 \oplus M_{12}$ . After computing  $M_{13}$ , then  $S_i$  verifies whether  $M_{13} = M_{11}$ . If it holds,  $S_i$  accepts  $C_i$ 's login request; otherwise,  $S_i$  rejects the login request.



### D. Password Change Phase.

In Jiping et al.'s scheme, user  $C_i$  can freely change the password  $PW_{oldi}$  to a new one  $PW_{newi}$ . The password change procedure is performed as follows.

(1)  $C_i$  inserts the smart card into the card reader and offers user's personal biometrics  $B'_i$ . The smart card computes  $f'_i =$

$h(B'_i)$  and verifies it by checking  $d(f'_i, f_i) \leq \tau$ . Where  $f_i = h(B_i)$  is the information stored in the smart card.

(2) If it holds,  $C_i$  inserts old password  $PW_{oldi}$  and new password  $PW_{newi}$ . Otherwise the password change procedure is terminated.

(3) Smart card performs  $r'_i = h(PW_{oldi}) \oplus f'_i$  and checks  $d(r'_i, r_i) \leq \tau$ .  $r_i$  is the information stored in the smart card.

(4) If it holds, the smart card computes  $r'_i = h(PW_{newi}) \oplus f_i$ ,  $e'_i = e_i \oplus r_i (= h(ID_i \| X_s))$ , and  $e''_i = e'_i \oplus r_i$ .

(5) Finally, replace  $e_i$  with  $e''_i$  and  $r_i$  with  $r''_i$  on the smart card.

#### IV. CRYPTANALYSIS OF JIPING ET AL.'S SCHEME

Jiping et al enhanced the security of Das's authentication scheme and proposed the new authentication scheme. But Jiping et al's authentication scheme still has security problem. These problems are server masquerading attack, stolen smart card attack and authentication without login phase.

##### A. Server Masquerading Attack

Attacker can masquerade as legitimate server if attacker knows  $h(g_i \| X_s)$ . It is reason that server authenticates user using only  $h(g_i \| X_s)$ . Figure 4 shows the phase of server masquerading attack. Firstly, attacker intercepts client's message  $\langle g_i, M_2, M_3, T \rangle$ . Then, attacker calculates  $h(g_i \| X_s)$  using  $M_2 \oplus M_3$ . Because  $h(g_i \| X_s) = e_i \oplus r_i = M_2 \oplus M_3$ . The attacker computes  $M_4, M_6, M_7$  and  $T_A$  using  $h(g_i \| X_s)$  and sends them to client. The client check and authenticate messages. And the attacker receives  $M_{11}, R_c$  and  $T'$ , then attacker checks the success to masquerades as server. The client is authenticated with the attacker. In Jiping et al's scheme, the attacker can execute server masquerading attack. To solve this problem, it is necessary to add another security information to authenticate with server and client. The Attacker has to not compute the security information using communicate message between server and client.

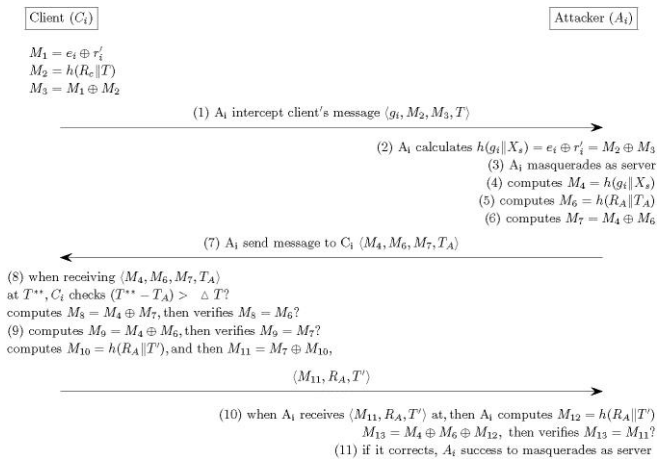


Fig. 4. Server Masquerading Attack

##### B. Stolen Smartcard Attack

Kocher et al. and Messerges et al. pointed out that the confidential information stored in all existing smart cards could be extracted by physically monitoring its power consumption. Therefore, if the user loses his smart card, all secrets in the smart card may be revealed by attacker [13,14].

In Jiping et al.'s scheme, a smart card stores various secrets

for the login and authentication of user. The smart card for user  $ID_i$  includes  $(h(\cdot), f_i, g_i, e_i, r_i, \tau, d(\cdot))$ . So if attacker gets or steals user's smart card, attacker can obtain and know  $f_i, g_i, r_i$  of user $_i$ . The attacker can calculate  $h(PW_i)$  and  $h(ID_i)$ , then attacker executes off-line password attack using rainbow table, dictionary attack and brute attack. So the attacker can obtain  $ID_i$  and  $PW_i$ . It is reason that  $ID_i$  and  $PW_i$  are protected using  $h(\cdot)$ . To solve this problem, it is necessary to add random number with high-entropy. Figure 5 shows the phase of stolen smart card attack.

Attacker

gets(steals) user's smart card

obtains information from smart card using SPA and DPA

→ gets  $h(\cdot), f_i, g_i, e_i, r_i, \tau$  and  $d(\cdot)$

Attacker knows  $f_i, g_i, r_i$

$r_i = h(PW_i) \oplus f_i$

→  $h(ID_i) = g_i$

→  $h(PW_i) = r_i \oplus f_i$

executes off-line password attack

→ figures out user's ID and password  $ID_i, PW_i$

Fig. 5. Stolen smart card attack

##### C. Authentication without Login Phase.

In Jiping et al.'s scheme, attacker can be authenticate with server without login phase. To skip the login phase, the attacker need to still or get the user's smart card. In other words, if the attacker obtain user's smart card, the attacker can be authenticate to server without user's  $ID_i, PW_i$  and user's biometric information  $B_i$ . Figure 6 shows the phase of authentication without login phase.

Attacker

gets(steals) user's smart card

obtains information from smart card using SPA and DPA

→ gets  $h(\cdot), f_i, g_i, e_i, r_i, \tau$  and  $d(\cdot)$

computes  $M_1, M_2, M_3$

→ generates random number  $R_c$

→  $M_1 = e_i \oplus r_i$

→  $M_2 = h(R_c \| T)$

→  $M_3 = M_1 \oplus M_2$

sends login and authentication message to  $S_i$

→  $\langle g_i, M_2, M_3, T \rangle$

receives  $S_i$ 's message

→  $\langle M_4, M_6, M_7, T_s \rangle$

computes  $M_{11}, R_c, T'$

→ generates timestamp  $T'$

→  $M_{10} = h(R_c \| T')$

→  $M_{11} = M_8 \oplus M_{10}$

sends authentication message to  $S_i$

→  $\langle M_{11}, R_c, T' \rangle$

→ attacker can be authenticated with  $S_i$

Fig. 6. Authentication without login phase

Firstly, attacker gets or steals the user's smart card and obtains information from smart card using SPA and DPA. So the attacker can generate and compute the  $R_c$ ,  $M_1$ ,  $M_2$  and  $M_3$  using this information. And the attacker sends  $\langle g_i, M_2, M_3, T \rangle$  to the server. Then, the attacker receives  $\langle M_4, M_6, M_7, T_s \rangle$  and then, the attacker can compute  $\langle M_{11}, R_c, T' \rangle$  and send these messages to server. So attacker can be authenticated to the server without user's  $ID_i$ ,  $PW_i$  and the user's biometric information  $B_i$ . To solve this problem, it is necessary to add information of user's  $PW_i$  or  $B_i$  to authentication messages.

## V. PROPOSED SCHEME

In this section, to solve Jiping et al's security problem, we propose security enhanced biometric-based user authentication Scheme for the C/S System.

### A. Proposed registration phase

The registration procedure of proposed scheme is described in Fig. 7

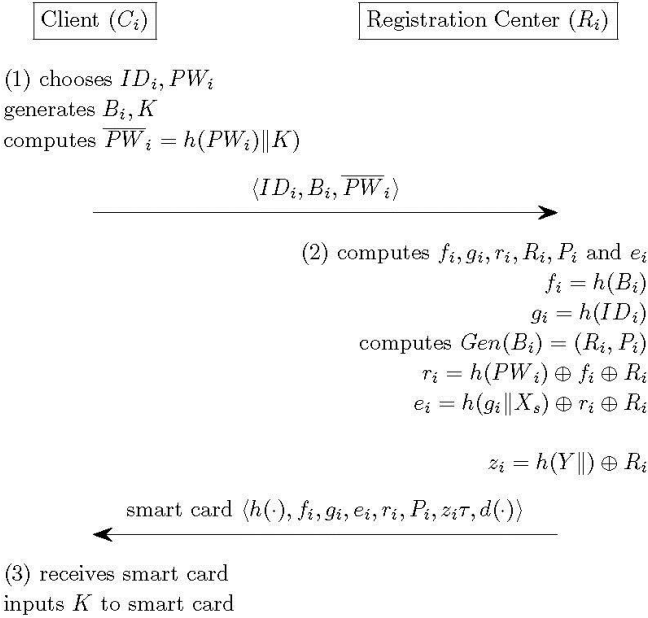


Fig. 7 Proposed Registration Phase

### B. Proposed login phase

And now, the login procedure of proposed scheme is described in Fig. 8

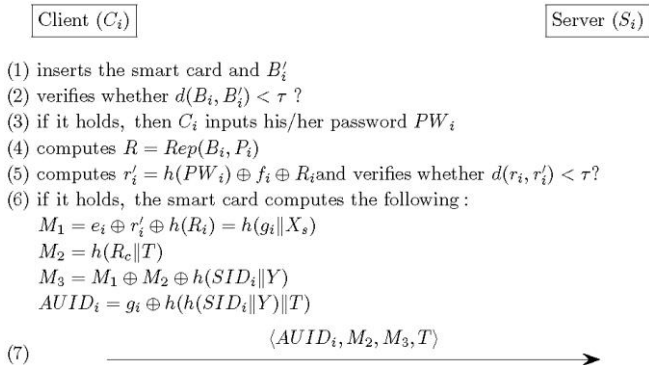


Fig. 8 Proposed Login Phase

### C. Proposed authentication phase

The authentication procedure of proposed scheme is described in Fig. 9

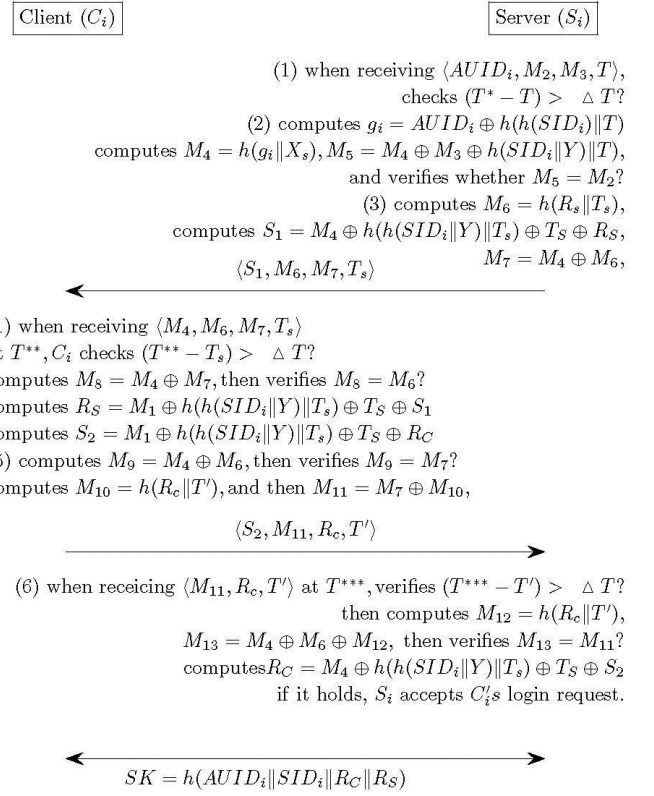


Fig. 9 Proposed Authentication Phase

## VI. CONCLUSION

In this paper, we analyze the cryptanalysis of Jiping et al.'s biometric-based user authentication scheme for the client/server system. Jiping et al. proposed an improved authentication scheme to solve the problem of vulnerabilities in Das's scheme. However, Jiping et al.'s scheme has some remaining security problems: the server-masquerading attack, stolen smart-card attack and authentication without login phase. To solve this problem, it is necessary to add secret information to the registration, login and authentication phases. And we proposed security enhanced biometric-based user authentication Scheme for the C/S System.

## REFERENCES

- [1] C. T. Li, "An enhanced remote user authentication scheme providing mutual authentication and key agreement with Smart Cards," in *Proceedings of the 5th International IEEE Computer Society Conference on Information Assurance and Security*, pp. 517-520, Xi'an, China, 2009.
- [2] K. H. M. Wong, Z. Yuan, C. Jiannong, and W. Shengwei, "A dynamic user authentication scheme for wireless sensor networks," in *Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC '06)*, pp. 244-251, Taichung, Taiwan, June 2006.
- [3] T. H. Lee, "Simple dynamic user authentication protocols for wireless sensor networks," in *Proceedings of the 2nd International Conference on Sensor Technologies and Application* pp.657-660, CapEstere, France, August 2008.
- [4] B. Vaidya, J. J. Rodrigues, and J. H. Park, "User authentication schemes with pseudonymity for ubiquitous sensor network in NGN," *International Journal of Communication Systems*, vol. 23, no. 9-10, pp. 1201-1222, 2010.

- [5] N.-Y. Lee and Y.-C. Chiu, "Improved remote authentication scheme with smart card," *Computer Standards and Interfaces*, vol. 27, no. 2, pp. 177–180, 2005.
- [6] M. Kim and C. K. Koc, "A simple attack on a recently introduced hash-based strong-password authentication scheme," *International Journal of Network Security*, vol. 1, no. 2, pp. 77–80, 2005..
- [7] L.-C. Ko, "A novel dynamic user authentication scheme for wireless sensor networks," in *Proceedings of the IEEE International Symposium on Wireless Communication Systems*, pp. 608–612, Reykjavik, Iceland, October 2008.
- [8] J. Nam, K. K. R. Choo, M. Kim, J. Paik and D. Won, "Dictionary Attacks against Password-Based Authenticated Three-Party Key Exchange Protocols", *KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS*, Volume 7, NO. 12, December 2013, pp.3244-3260.
- [9] J. Nam, K. K. R. Choo, J. Kim, Kang, H. K. Kim, J. Paik, and D. Won (2014). Password-Only Authenticated Three-Party Key Exchange with Provable Security in the Standard Model. *The Scientific World Journal*, 2014.
- [10] H. Jeong, D. Won and S. Kim, "Weaknesses and Improvement of Secure Hash-Based Strong-Password Authentication Protocol", *Journal of Information Science and Engineering*, Volume 26, Number 5, September 2010, pp.1845-1858.
- [11] A. K. Das, "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards." *Information Security*, IET 5.3 (2011): 145-151.
- [12] L. Jiping, D. Yaoming, X. Zenggang, and L. Shouyin, "An Improved Biometric-Based User Authentication Scheme for C/S System", *International Journal of Distributed Sensor Networks*, 2014.
- [13] P. Kocher, J. Jaffe, B. Jun, "Differential power analysis", *the 19th Annual International Cryptology Conference on Advances in Cryptology*, 1999, 388-397.
- [14] T. S. Messerges,; E. A. Dabbish, R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks", *Computers. IEEE Transactions on Computers*, 2002, 51(5), 541-552
- [15] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks. *IEEE Transactions on Computers*, 51(5), 541-552