*International Journal of Internet, Broadcasting and Communication Vol.8 No.3 50-57 (2016)*
*http://dx.doi.org/10.7236/IJIBC.2016.8.3.50*

IJIBC 16-3-6

# An Improved Biometrics-based Password Authentication Scheme with Session Key Agreement

Hyungkyu Yang

*Computer Media Information Engineering, Kangnam University,*
*111, Gugal-dong, Giheung-gu, Yongin-si, Gyounggi-do, 446-702, Korea*
*hkyang@kangnam.ac.kr*

***Abstract***

*In 2013, Li et al. proposed an improved smart card-based remote user password authentication scheme, and claimed that their scheme not only overcomes security weaknesses of the Chen et al.'s scheme but also is a more user friendly scheme compared with other schemes. In this paper, we analyze the security of Li et al.'s authentication scheme and we show that Li et al.'s authentication scheme is still insecure against the various attacks, such as the off-line password guessing attack, the forgery attack, and the session key generation attack etc. Also, we propose an improved scheme that can resist these security drawbacks of Li et al.'s authentication, even if the secret information stored in the smart card is revealed. As a result of security analysis, the improved scheme is relatively more secure against several attacks than other related schemes in terms of the security.*

**Keywords:** *Authentication, Biometrics, Password, Smart Card, Session Key Agreement*

## 1. Introduction

Recently, user authentication scheme in m-commerce has been becoming one of important security issues. Since Lamport [1], in 1987, first proposed a remote password authentication protocol with the insecure communication, many researchers [2-9] have proposed the improved authentication protocols to improve various kinds of security problems.

In traditional identity-based remote user authentications, the security of user authentication is based on the passwords, but simple passwords are easy to break by simply dictionary attacks. To resolve the simple password problems, many biometrics-based remote user authentication schemes [10-12] have been proposed.

Generally, biometrics-based remote user authentication is inherently more secure and reliable than the traditional authentication scheme. There are some advantages of using biometrics keys as compared to traditional passwords.

Manuscript Received: Jun. 17, 2016 / Revised: Jun. 27, 2016 / Accepted: Jul. 21, 2016
Corresponding Author: hkyang@kangnam.ac.kr
Tel: +82-31-280-3760
Dept. of Computer Media Information Engineering, Kangnam University

- Biometric keys cannot be lost or forgotten.
- Biometric keys are very difficult to copy or share.
- Biometric keys are extremely hard to forge or distribute.
- Biometric keys cannot be guessed easily.
- Someone's biometrics is not easy to break than others.

In 2013, Chen et al.'s [8] pointed out the weaknesses of some password authentication schemes [5-6] and proposed a robust smart card-based remote user password authentication scheme to improve the security. And they claim that their scheme is efficient and can ensure forward secrecy of the session key. However, Li et al. [9], in 2013, pointed out that Chen et al.'s scheme cannot really ensure forward secrecy, and it cannot detect the wrong password in the login phase. Besides the password change phase of Chen et al.'s scheme is unfriendly and inefficient. Then, Li et al. proposed an improved smart card-based remote user password authentication scheme, and they claimed that their scheme not only overcomes security weaknesses of the Chen et al.'s scheme but also is a more user friendly scheme compared with other schemes.

In this paper, we analyze the security of Li et al.'s smart card-based remote user password authentication scheme. And we show that Li et al.'s authentication scheme is still vulnerable to the various attacks, such as the off-line password guessing attack, the forgery attack, and the session key generation attack etc. Also, we propose the improved biometrics-based password authentication scheme to remove the security drawbacks of Li et al.'s authentication scheme, even if the secret information stored in the smart card is revealed. To analyze the security of the improved authentication scheme, we assume that an attacker can extract the values stored in the smart card by monitoring the power consumption [13-14] and intercept messages communicating between the user and the server.

This paper is organized as follows. In Section 2, we briefly review Li et al.'s scheme. In Section 3, we describe the security analysis of Li et al.'s scheme. The improved scheme is described in Section 4, and its security analysis is given in Section 5. Finally, conclusions are described in Section 6.

## 2. Reviews of Li et al.' Scheme

In 2014, Mishra et al. [11] proposed an improved biometrics-based remote user authentication scheme for telecare medicine information systems (TMIS). This scheme is composed of three phases: registration phase, login phase, and authentication phase. The notations used in this paper are as follows.

**Table 1. Notations used in this paper**

| Notation | Description |
|---|---|
| $U_i$ | User i |
| S | Authentication server |
| $ID_i$ | Identity of the user i |
| $PW_i$ | Password of the user i |
| $Bio_i$ | Biometrics template of the user i |
| x | Master secret key hold by server S |
| h() | A secure hash function |
| $x \| y$ | x concatenates with y |
| $x \oplus y$ | Exclusive-OR operation of x and y |

### 2.1 Registration Phase

Before accessing the system, a user $U_i$ initially needs to register with an authentication server S as the following steps.

R1. $U_i$ submits his identity $ID_i$ and password $PW_i$ to S via secure channel.

R2. S computes $A_i=h(ID_i \| PW_i)^{PW_i}$ mod p, and $B_i=h(ID_i)^{(x+PW_i)}$ mod p.

R3. S stores personal security parameters ($A_i$, $B_i$, h(), p, q) on the user's smart card and issues the smart card to $U_i$ via secure channel.

### 2.2 Login Phase

When the user $U_i$ wants to login to the authentication server S, the user has to perform the following steps.

L1. $U_i$ inputs $ID_i$ and $PW_i$, and then the smart card computes $A_i^*=h(ID_i \| PW_i)^{PW_i}$ mod p. If $A_i^*$ equals $A_i$, the smart card computes the following equations, where $\alpha$is a random number chosen by the user and $T_i$ is a current timestamp of the user. Otherwise, the smart card terminates the session.

$C_i=B_i/h(ID_i)^{PW_i}$ mod p

$D_i=h(ID_i)^{\alpha}$ mod p

$M_i=h(ID_i \| C_i \| D_i \| T_i)$

L3. $U_i$ sends the login request message $\{ID_i, D_i, M_i, T_i\}$ to S.

### 2.3 Authentication Phase

After receiving the login request message, the authentication server S has to perform the following steps to authenticate between the user and the server.

A1. S checks that $ID_i$ is valid and that $(T_i^{'}-T_i)\leq\Delta T$, where $T_i^{'}$ is the time when the login request message is received. If they are valid, S performs the following equations.

$C_i^*=h(ID_i)^x$ mod p

$M_i^*=h(ID_i \| C_i^* \| D_i \| T_i)$

A2. S checks whether $M_i=M_i^*$ or not. If they are equal, S accepts the user's login request message, and the user is authenticated by the authentication server.

A3. Then, S computes the following equations, where $\beta$ is a random number chosen by the server and $T_s$ is a current timestamp of the server.

$V_i=h(ID_i)^{\beta}$mod p

$sk=D_i^{\beta}$mod p

$M_s=h(ID_i \| C_i^{'} \| V_i \| D_i \| sk \| T_s)$

A4. S sends the mutual authentication message $\{ID_i, V_i, M_s, T_s\}$ to $U_i$.

A5. After receiving the mutual authentication message, $U_i$ checks that the $ID_i$ is valid and that $(T_s^{'}- T_s)\leq\Delta T$, where $T_s^{'}$ is the time when the mutual authentication message is received. If they are valid, $U_i$ computes the following equations.

$sk^*= V_i^{\alpha}$ mod p

$M_s^*=h(ID_i \| C_i \| V_i \| D_i \| sk^* \| T_s)$

A6. $C_i$ checks whether $M_s^*=M_s$ or not. If they are equal, $U_i$ accepts the mutual authentication message, and the authentication server is authenticated by the user.

A7. After achieving mutual authentication, they can compute the shared session key $sk=V_i^{\alpha}$ mod $p=D_i^{\beta}$ mod $p=h(ID_i)^{\alpha\beta}$ mod p respectively for secrecy communication.

## 3. Attacks against of Li et al.' Scheme

In this section, we will discuss the security drawbacks of Li et al.'s smart card based authentication scheme. To analyze Li et al.'s scheme, we assume that an attacker could obtain the secret values stored in the smart card by monitoring the power consumption and intercept messages communicating between the user and the server [13-14]. Under this assumption, we will discuss the various attacks, such as the off-line password guessing attack, the forgery attack, and the session key generation attack etc.

### 3.1 Password Guessing Attack

If an attacker can extract the secret values ($A_i$) from the legal user's smart card by some means, the attacker can easily find out $PW_i$ by the following steps, where $PW_i^*$ is the guessed password.

PA1. The attacker computes $A_i^*=h(ID_i \parallel PW_i^*)^{PWi*}$ mod p from the registration phase.

PA2. The attacker verifies the correctness of $PW_i^*$ by checking $A_i=A_i^*$.

PA3. The attacker repeats the above steps until a correct password $PW_i^*$ is found.

Finally, the attacker can get the correct password by performing the off-line password guessing attack, and can perform successfully the various attacks with the guessed password.

### 3.2 Forgery Attack

With the extracted secret values ($B_i$) from the legal user's smart card and the guessed password $PW_i^*$ in subsection 3.1, the attacker can easily perform the user impersonation attack as the following steps.

FA1. The attacker computes the following equations, where γ is a random number chosen by the attacker.

$C_i^*=B_i/h(ID_i)^{PWi*}\text{mod } p$

$D_i^*=h(ID_i)^{\gamma}\text{mod } p$

$M_i^*=h(ID_i \parallel C_i^* \parallel D_i^* \parallel T_a)$

where $T_a$ is a current timestamp of the attacker.

FA2. Then, the attacker sends the forged login request message $\{ID_i, D_i^*, M_i^*, T_a\}$ to the authentication server S.

FA3. Upon receiving the forged message, S checks whether $ID_i$ and $(T_s'-T_s)\leq\Delta T$ are valid or not, where $T_s'$ is the time when the forged login request message is received. If they are valid, S performs the following equations.

$C_i'=h(ID_i)^x \text{ mod } p$

$M_i^*=h(ID_i \parallel C_i' \parallel D_i^* \parallel T_a)$

FA4. S checks whether $M_i=M_i^*$ or not. If they are equal, the attacker is authenticated by the authentication server.

Also, with the extracted secret values ($B_i$), the guessed password $PW_i^*$ and the intercepted massage ($D_i$), the attacker can perform the server masquerading attack by sending the forged mutual authentication message $\{ID_i, V_i^*, M_s^*, T_a^*\}$ to the user.

$V_i^*=h(ID_i)^{\delta}\text{mod } p$

$sk^*= D_i^{\delta}\text{mod } p$

$M_s^*=h(ID_i \parallel C_i^* \parallel V_i^* \parallel D_i \parallel sk^* \parallel T_a^*)$

where δ is a random number chosen by the attacker.

### 3.3 Session Key Gneration Attack

Generally, the shared session key generation is provided for secure communication of messages between the server and the user. In the Li et al.'s scheme, the attacker can establish the shared session key $sk^*=h(ID_i)^{\alpha\delta}$mod p by performing the server masquerading attack or $sk^*=h(ID_i)^{\gamma\beta}$mod p by performing the user impersonation attack as shown in subsection 3.2 if the attacker can obtain the secret values stored in the smart card and intercept messages communicating between the server and the user. Thus, we can see that the Li et al.'s scheme does not resist the session key generation attack.

## 4. The Improved Scheme

In this section, we propose an improved d biometrics-based password authentication scheme, which keeps the merits of the Li et al.'s scheme and withstands the various attacks, such as the password guessing attack, the forgery attack, the replay attack, etc. Also, the improved scheme achieves the session key generation via mutual authentication. The improved scheme is divided into three phases: registration phase, login phase and authentication phase.

In order to initialize the scheme, the authentication server S selects large prime number p and q such that p=2q+1, then S chooses the master secret key $x \in Z_q$.

### 4.1 Registration Phase

Before accessing the system, a user $U_i$ initially needs to register with the authentication server S as the following steps. The registration phase is illustrated in figure 1.

R1. $U_i$ submits his identity $ID_i$, password information $(PW_i \oplus R)$ and biometrics information $(Bio_i \oplus R)$ to S via secure channel, where R is a random number generated by $U_i$.

R2. S computes the following equations.

$$f_i=(PW_i \oplus Bio_i)$$

$$A_i=h(ID_i \parallel f_i)^{(PWi \oplus R)} \bmod p$$

$$B_i=h(ID_i)^{(x+(PWi \oplus R))} \bmod p$$

R3. S stores personal security parameters ($A_i$, $B_i$, h(), p, q) on a user's smart card and issues the smart card to $U_i$ via secure channel. And $U_i$ stores random number R into the smart card.

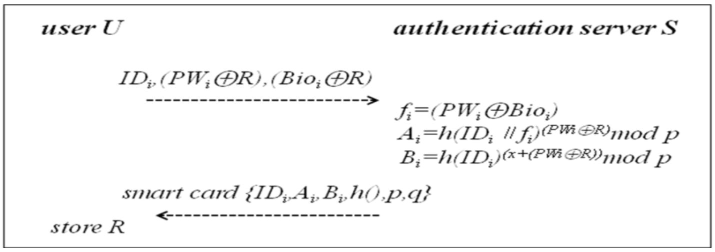
user U
authentication server S
$ID_i, (PW_i \oplus R), (Bio_i \oplus R)$
$f_i=(PW_i \oplus Bio_i)$
$A_i=h(ID_i \,//\, f_i)^{(PWi \oplus R)} mod\ p$
$B_i=h(ID_i)^{(x+(PWi \oplus R))} mod\ p$
smart card $\{ID_i, A_i, B_i, h(), p, q\}$
store R

**Figure 1. Registration phase of the improved scheme**

### 4.2 Login Phase

When the user $U_i$ wants to login to the authentication server S, the user has to perform the following steps. The login phase and authentication phase is illustrated in figure 2.

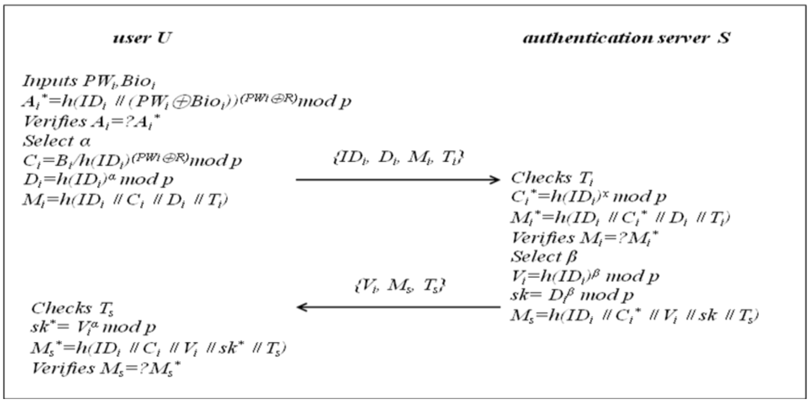
user U
authentication server S
Inputs $PW_i, Bio_i$
$A_i^*=h(ID_i \,//\, (PW_i \oplus Bio_i))^{(PWi \oplus R)} mod\ p$
Verifies $A_i=?A_i^*$
Select $\alpha$
$C_i=B_i/h(ID_i)^{(PWi \oplus R)} mod\ p$
$D_i=h(ID_i)^{\alpha}\ mod\ p$
$M_i=h(ID_i \,//\, C_i \,//\, D_i \,//\, T_i)$
$\{ID_i,\ D_i,\ M_i,\ T_i\}$
Checks $T_i$
$C_i^*=h(ID_i)^x\ mod\ p$
$M_i^*=h(ID_i \,//\, C_i^* \,//\, D_i \,//\, T_i)$
Verifies $M_i=?M_i^*$
Select $\beta$
$V_i=h(ID_i)^{\beta}\ mod\ p$
$sk= D_i^{\beta}\ mod\ p$
$M_s=h(ID_i \,//\, C_i^* \,//\, V_i \,//\, sk \,//\, T_s)$
$\{V_i,\ M_s,\ T_s\}$
Checks $T_s$
$sk^*= V_i^{\alpha}\ mod\ p$
$M_s^*=h(ID_i \,//\, C_i \,//\, V_i \,//\, sk^* \,//\, T_s)$
Verifies $M_s=?M_s^*$

**Figure 2. Login phase and authentication phase of the improved scheme**

L1. $U_i$ inputs $ID_i$ and $PW_i$, and biometrics information $Bio_i$ and then the smart card computes $A_i^*=h(ID_i \,||\, h(PW_i \oplus Bio_i))^{(PW_i \oplus R)} \bmod p$. If $A_i^*$ equals $A_i$, the smart card computes the following equations. Otherwise, the smart card terminates the session.

$C_i=B_i/h(ID_i)^{(PW_i \oplus R)} \bmod p$

$D_i=h(ID_i)^{\alpha} \bmod p$

$M_i=h(ID_i \,||\, C_i \,||\, D_i \,||\, T_i)$

where $\alpha$ is a random number chosen by the user and $T_i$ is a current timestamp of the user.

L3. $U_i$ sends the login request message $\{ID_i, D_i, M_i, T_i\}$ to S.

### 4.3 Authentication Phase

After receiving the login request message, the authentication server S has to perform the following steps to authenticate between the user and the authentication server.

A1. S checks that the $ID_i$ is valid and that $(T_i^{'}-T_i) \le \Delta T$, where $T_i^{'}$ is the time when the login request message is received. If they are valid, S performs the following equations.

$C_i^*=h(ID_i)^x \bmod p$

$M_i^*=h(ID_i \,||\, C_i^* \,||\, D_i \,||\, T_i)$

A2. S checks whether $M_i=M_i^*$ or not. If they are equal, S accepts the user's login request message, and the user is authenticated by the authentication server.

A3. Then, S computes the following equations, where $\beta$ is a random number chosen by the server and $T_s$ is a current timestamp of the server.

$V_i=h(ID_i)^{\beta} \bmod p$

$sk= D_i^{\beta} \bmod p$

$M_s=h(ID_i \,||\, C_i^* \,||\, V_i \,||\, D_i \,||\, sk \,||\, T_s)$

A4. S sends the mutual authentication message $\{V_i, M_s, T_s\}$ to $U_i$.

A5. After receiving the mutual authentication message, $U_i$ checks that $(T_s^{'} - T_s) \le \Delta T$, where $T_s^{'}$ is the time when the mutual authentication message is received. If they are valid, $U_i$ computes the following equations.

$sk^*= V_i^{\alpha} \bmod p$

$M_s^*=h(ID_i \,||\, C_i \,||\, V_i \,||\, D_i \,||\, sk^* \,||\, T_s)$

A6. $U_i$ checks whether $M_s^*=M_s$ or not. If they are equal, $U_i$ accepts the mutual authentication message, and the authentication server is authenticated by the user.

A7. After achieving mutual authentication, they can compute the shared session key $sk=V_i^{\alpha} \bmod p=D_i^{\beta} \bmod p=h(ID_i)^{\alpha\beta} \bmod p$ respectively for secrecy communication.

## 5. Security Analysis of the Improved Scheme

In this section, we will discuss the security of the improved scheme based on the password and biometrics information. To analyze the security of the improved scheme, we assume that an attacker can extract the secret values stored in the smart card by monitoring the power consumption [13-14] and intercept the messages communicating between the user and the server. Under this assumption, we will discuss the various attacks, such as the off-line password guessing attack, the forgery attack, the replay attack and the session key generation attack etc.

### 5.1 Password Guessing Attack

With the extracted secret values ($A_i$, $B_i$, h(), p, q) from the legal user's smart card and the intercepted messages {$ID_i$, $D_i$, $M_i$, $T_i$}, {$V_i$, $M_s$, $T_s$} communicating between the user and the server, the attacker may attempt to guess the user's password $PW_i$ computing $A_i$ or $B_i$ in the registration phase. However, the attacker cannot guess the user's password $PW_i$ without knowing the biometrics information $Bio_i$ generated by the user and the master secret value x kept by the server.

### 5.2 Forgery Attack

To impersonate as the legal user, an attacker may attempt to make a forged login request message {$ID_i$, $D_i^*$, $M_i^*$, $T_a$}. However, the attacker cannot compute the forged login request message without knowing the master secret value x, the user's password $PW_i$ and the random number $\alpha$, even if the attacker can extract the secret values ($A_i$, $B_i$) stored in the user's smart card. Hence, the attacker cannot impersonate as the legal user to the server by performing the user impersonation attack.

Also, to masquerade as the legitimate server, an attacker may attempt to make the forged mutual authentication massage {$V_i^*$, $M_s^*$, $T_s$} when receiving the user's login request message. However, the attacker cannot compute the forged mutual authentication massage without knowing the master secret value x and the random number $\beta$, even if the attacker can extract the secret values ($A_i$, $B_i$) stored in the user's smart card. Hence, the attacker cannot masquerade as the legitimate server to the user by performing the server masquerading attack.

### 5.3 Replay Attack

The attacker may replay the previously used login request message and mutual authentication massage to cheat the user or the authentication server. However, in the improved scheme, the timestamp $T_i$ in the login request message and the timestamp $T_s$ in the mutual authentication massage are updated on new timestamp whenever new session is started. Therefore, the replayed messages can be detected by checking the timestamp. So, the improved scheme can resist the replay attack.

### 5.4 Session Key Generation Attack

With the extracted secret values ($A_i$, $B_i$) from the legal user's smart card and the intercepted messages {$ID_i$, $D_i$, $M_i$, $T_i$}, {$V_i$, $M_s$, $T_s$} communicating between the user and the server, the attacker may attempt to compute the shared session key sk. However, the attacker cannot compute the shared session key $sk=V_i^{\alpha} \bmod p=D_i^{\beta} \bmod p=h(ID_i)^{\alpha\beta} \bmod p$ without knowing the master secret value x kept by the server, the random number $\alpha$ generated by the user and the random number $\beta$ generated by the authentication server. Thus, the improved scheme can resist the session key generation attack.

### 5.5 Security Comparisons of the Improved Scheme and Other Related Scheme

The security comparison of the improved scheme and other related schemes are summarized in Table 2. As a result, the improved scheme is relatively more secure against several attacks than other related schemes.

**Table 2. Security Comparison of the Improved Scheme and Other Related Scheme**

| security features | Chen's scheme [8] | Li et al.'s scheme [9] | Improved scheme |
|---|---|---|---|
| password guessing attack | impossible | possible | impossible |
| forgery attack | impossible | possible | impossible |
| replay attack | impossible | impossible | impossible |
| session key generation attack | impossible | possible | impossible |
| insider attack | possible | possible | impossible |

## 6. Conclusions

In this paper, we point out that the Li et al.'s scheme is not secure against the various attacks, such as the off-line password guessing attack, the forgery attack and the session key generation attack etc. Also, we proposed the improved scheme that resist the password guessing attack, the forgery attack, the replay attack, the insider attack and the session key generation attack etc., even if the secret information stored in the smart card is revealed. As a result of security comparison, the improved scheme is relatively more secure against several attacks than other related schemes in terms of the security.

## Acknowledgement

This work was supported by Kangnam University Research Grants.(2014)

## References

[1] L. Lamport, “Password Authentication with Insecure Communication,” Communications of the ACM, vol. 24, no. 11, pp. 770-772, 1987.

[2] S.M. Woo and M. Lee,” Sensors Network and Security and Multimedia Enhancement,” The International Journal of Internet, Broadcasting and Communication(IJIBC), Vol. 8, No. 1, pp. 64-76, Feb 2016.

[3] J.J. Kim, J.J. Kang, E.J. Rothwell and K.Y. Lee,” RFID-based Secure Communication for Smart Device in Future Home Network Environment,” The International Journal of Internet, Broadcasting and Communication(IJIBC), Vol. 5, No. 1, pp. 18-22, May 2013.

[4] Liu, J.Y., Zhou, A.M., Gao, M.X,” A New Mutual Authentication Scheme based on Nonce and Smart Cards,” Computer Communications, vol. 31, pp. 2205-2209, 2008.

[5] Xu, J., Zhu, W.T., Feng, D.G.,” An Improved Smart Card-based Remote User Password Authentication Scheme with Provable Security,” Computer Standards and Interfaces, vol. 31, no. 4, pp. 723-728, 2009.

[6] Sood, S.K., Sarje, A.K., Singh, K.,” An Improvement of Xu et al.'s Authentication Scheme using Smart Cards,” Proceedings of the 3rd annual ACM Bangalore conference, India, pp. 17-5, 2010.

[7] Awasthi, A.K., Srivastava, K., Mittal, R.C,” An Improved Timestamp-based Remote User Authentication Scheme,” Computer and Electrical Engineering, vol. 37, pp. 869-874 (2011)

[8] Chen, B.L., Kuo, W.C., WCC, L.C.: Robust Smart Card-based Remote User Password Authentication Scheme. International Journal of Communication Systems, 2013.

[9] Xiong, L., Jianwei, N., Muhammad, K.K., Junguo, L.,” An Enhanced Smart Card-based Remote User Password Authentication Scheme,” Journal of Network and Computer Applications, vol. 36, pp. 1365-1371, 2013.

[10] Khan, M.K., Zhang, J.,” An Efficient and Practical Fingerprint-based Remote User Authentication Scheme with Smart Cards,” ISPEC 2006, LNCS 3903, pp. 260-268, 2006.

[11] Li, C.T., Hwang, M.S.,” An Efficient Biometrics-based Remote User Authentication Scheme Using Smart Cards,” Journal of Network and Computer Applications, vol. 33, pp. 1-5, 2010.

[12] Das, A.K.,” Analysis and Improvement on an Efficient Biometric-based Remote User Authentication Scheme Using Smart Cards,” IET Information Security, vol.5, Iss. 3, pp. 541-552, 2011.

[13] Kocher, P., Jaffe, J., Jun, B.,” Differential Power Analysis,” Proceedings of Advances in Cryptology, pp. 388-397, 1999.

[14] 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, vol. 51, no. 5, pp. 541-552, 2002.