Hindawi Publishing Corporation
Journal of Biomedicine and Biotechnology
Volume 2012, Article ID 519723, 6 pages
doi:10.1155/2012/519723

*Research Article*

# Security Analysis and Enhancements of an Effective Biometric-Based Remote User Authentication Scheme Using Smart Cards

**Younghwa An**

*Division of Computer and Media Information Engineering, Kangnam University, 111, Gugal-dong, Giheung-gu, Yongin-si, Gyounggi-do, 446-702, Republic of Korea*

Correspondence should be addressed to Younghwa An, yhan@kangnam.ac.kr

Received 25 May 2012; Accepted 7 June 2012

Academic Editor: Sabah Mohammed



Recently, many biometrics-based user authentication schemes using smart cards have been proposed to improve the security weaknesses in user authentication system. In 2011, Das proposed an efficient biometric-based remote user authentication scheme using smart cards that can provide strong authentication and mutual authentication. In this paper, we analyze the security of Das's authentication scheme, and we have shown that Das's authentication scheme is still insecure against the various attacks. Also, we proposed the enhanced scheme to remove these security problems of Das's authentication scheme, even if the secret information stored in the smart card is revealed to an attacker. As a result of security analysis, we can see that the enhanced scheme is secure against the user impersonation attack, the server masquerading attack, the password guessing attack, and the insider attack and provides mutual authentication between the user and the server.

## 1. Introduction

Recently, user authentication scheme in e-commerce and m-commerce has become one of important security issues. However, the security weaknesses in the remote user authentication scheme have been exposed seriously due to the careless password management and the sophisticated attack techniques. Several schemes [1–6] have been proposed to enhance the various security problems in user authentication schemes.

In traditional identity-based remote user authentications, the security of the remote user authentication is based on the passwords, but simple passwords are easy to break by simple dictionary attacks. To resolve the single-password authentication problems, several biometrics-based remote user authentication schemes [7–13] have been designed. 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.

(i) Biometric keys cannot be lost or forgotten.

(ii) Biometric keys are very difficult to copy or share.

(iii) Biometric keys are extremely hard to forge or distribute.

(iv) Biometric keys cannot be guessed easily.

(v) Someone's biometrics is not easy to break than others.

In 2010, Li and Hwang [12] proposed an efficient biometrics-based remote user authentication scheme using smart cards. They claimed that their scheme not only keeps good properties (e.g., without synchronized clock, freely changes password, mutual authentication) but also provides nonrepudiation. But Das [13], in 2011, pointed out that Li-Hwang's scheme does not resolve security drawbacks in login and authentication, security drawbacks in password change phase, and security drawbacks in verification of biometrics. Then, Das proposed more efficient biometrics-based remote user authentication scheme using smart cards which is secure against the user impersonation attack, the server masquerading attack, the parallel session attack, and the stolen password attack, and provide mutual authentication.

In this paper, we analyze the security of Das's authentication scheme, and we have shown that Das's authentication scheme is still vulnerable to the various attacks and does not provide mutual authentication between the user and the server. Also, we proposed the enhanced scheme to remove these security problems of Das's authentication scheme, even if the secret information stored in the smart card is revealed to an attacker. To analyze the security analysis of Das's authentication scheme, we assume that an attacker could obtain the secret values stored in the smart card by monitoring the power consumption [14, 15] and intercept messages communicating between the user and the server. Also, we assume that an attacker may possess the capabilities to thwart the security schemes.

(a) An attacker has total control over the communication channel between the user and the server in the login and authentication phase. That is, the attacker may intercept, insert, delete, or modify any message across the communication procedures.

(b) An attacker may (i) either steal a user's smart card and then extract the secret values stored in the smart card, (ii) or steal a user's password, but cannot commit both of (i) and (ii) at a time.

Obviously, if both of the user's smart card and password was stolen at the same time, then there is no way to prevent an attacker from impersonating as the user. Therefore, a remote user authentication scheme should be secure if only one case out of (i) and (ii) is happening.

This paper is organized as follows. In Section 2, we briefly review Das's authentication scheme. In Section 3, we describe the security analysis of Das's authentication scheme. The enhanced scheme is presented in Section 4, and security analysis of the enhanced scheme is given in Section 5. Finally, the conclusions are presented in Section 6.

## 2. Reviews of Das's Scheme

In 2011, Das proposed an improved biometrics-based remote user authentication scheme using smart cards. This scheme is composed of three phases: registration phase, login phase, and authentication phase. The notations used in this paper are as follows shown in Table 1.

*2.1. Registration Phase.* Before logging in the remote server $S_i$, a user $C_i$ initially has to register to the trusted registration centre $R_i$ as the following steps.

(R1) $C_i$ submits his identity $\mathrm{ID}_i$ and password $\mathrm{PW}_i$ to $R_i$ through a secure channel. Also, the user submits his biometrics information $B_i$ on the specific device to $R_i$.

(R2) $R_i$ computes $f_i = h(B_i)$, $r_i = h(\mathrm{PW}_i) \oplus f_i$ and $e_i = h(\mathrm{ID}_i \| X_s) \oplus r_i$, where $X_s$ is a secret value generated by the server.

(R3) $R_i$ stores $(\mathrm{ID}_i, h(), f_i, e_i, r_i)$ on the user's smart card and sends it to the user via a secure channel.

Table 1: Notations used in this paper.

| Notation | Description |
|---|---|
| $C_i$ | User $i$ |
| $R_i$ | Trusted registration centre $i$ |
| $S_i$ | Server $i$ |
| $A_i$ | Attacker $i$ |
| $\mathrm{PW}_i$ | Password of the user $i$ |
| $\mathrm{ID}_i$ | Identity of the user $i$ |
| $B_i$ | Biometric template of the user $i$ |
| $h(\,)$ | A secure hash function |
| $X_s$ | A secret information maintained by the server |
| $x \| y$ | $x$ concatenates with $y$ |
| $x \oplus y$ | Exclusive-OR operation of $x$ and $y$ |

*2.2. Login Phase.* When the user $C_i$ wants to log in the remote server $S_i$, the user has to perform the following steps.

(L1) $C_i$ inserts his smart card into a card reader and inputs the personal biometrics information $B_i$ on the specific device to verify the user's biometrics. If the biometrics information matches the template stored in the system, $C_i$ passes the biometrics verification.

(L2) $C_i$ inputs the $\mathrm{ID}_i$ and $\mathrm{PW}_i$, and then the smart card computes $r_i' = h(\mathrm{PW}_i) \oplus f_i$. If $r_i'$ equals $r_i$, the smart card computes the following equations, where $R_c$ is a random number generated by the smart card:

$$M_1 = e_i \oplus r_i'$$
$$M_2 = M_1 \oplus R_c \quad (1)$$
$$M_3 = h(R_c)$$

(L3) $C_i$ sends the login request message $\{\mathrm{ID}_i, M_2, M_3\}$ to $S_i$.

*2.3. Authentication Phase.* After receiving the request login message, the remote server $S_i$ has to perform the following steps with the user $C_i$ to authenticate each other.

(A1) $S_i$ checks the format of $\mathrm{ID}_i$.

(A2) If the $\mathrm{ID}_i$ is valid, $S_i$ computes $M_4 = h(\mathrm{ID}_i \| X_s)$ and $M_5 = M_2 \oplus M_4$.

(A3) $S_i$ verifies whether $M_3 = h(M_5)$ or not. If they are equal, $S_i$ computes the following equations, where $R_s$ is a random number generated by the server:

$$M_6 = M_4 \oplus R_s,$$
$$M_7 = h(M_2 \| M_5), \quad (2)$$
$$M_8 = h(R_s).$$

(A4) Then, $S_i$ sends the message $\{M_6, M_7, M_8\}$ to $C_i$.

(A5) After receiving the reply message, $C_i$ verifies whether $M_7 = h(M_2 \| R_c)$ or not. If they are equal, $C_i$ computes $M_9 = M_6 \oplus M_1$.

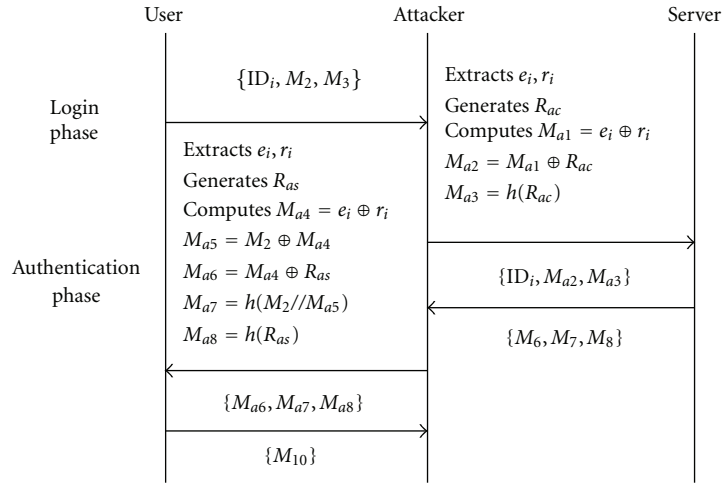


Figure 1: User impersonation attack and server masquerading attack.

(A6) $C_i$ verifies whether $M_8 = h(M_9)$ or not. If they are equal, $C_i$ computes $M_{10} = h(M_6 \| M_9)$.

(A7) Then, $C_i$ sends the message $\{M_{10}\}$ to $S_i$.

(A8) After receiving the message, $S_i$ verifies whether $M_{10} = h(M_6 \| R_s)$ or not. If they are equal, $S_i$ accepts the user's login request.

## 3. Security Analysis of Das's Scheme

In this section, we will analyze the security of Das's scheme. To analyze the security weaknesses, we assume that an attacker could obtain the secret values stored in the smart card by monitoring the power consumption [14, 15] and intercepting messages communicating between the user and the server. Under this assumption, we will discuss the various attacks, such as the user impersonation attack, the server masquerading attack, the password guessing attack, the insider attack, and the mutual authentication between the user and the server.

*3.1. User Impersonation Attack.* If the attacker can obtain the secret values $(e_i, r_i)$ from the user's smart card illegally by some means and intercept the message $\{\mathrm{ID}_i, M_2, M_3\}$ in the login phase, the attacker can perform the user impersonation attack as the following steps. The procedure of the user impersonation attack is illustrated in Figure 1.

(UA1) The attacker $A_i$ computes the following equations, where $R_{ac}$ is a random number chosen by the attacker:

$$\begin{aligned} M_{a1} &= e_i \oplus r_i, \\ M_{a2} &= M_{a1} \oplus R_{ac}, \\ M_{a3} &= h(R_{ac}). \end{aligned} \tag{3}$$

(UA2) Then, $A_i$ sends the forged message $\{\mathrm{ID}_i, M_{a2}, M_{a3}\}$ to the remote server $S_i$.

(UA3) Upon receiving the forged message, $S_i$ checks the format of $\mathrm{ID}_i$. If it holds, $S_i$ computes $M_4 = h(\mathrm{ID}_i \| X_s)$ and $M_5 = M_{a2} \oplus M_4$.

(UA4) $S_i$ verifies whether $M_{a3} = h(M_5)$ or not. If they are equal, $S_i$ will be convinced the message $\{\mathrm{ID}_i, M_{a2}, M_{a3}\}$ sent from the legal user.

(UA5) Then, $S_i$ makes the reply message $\{M_6, M_7, M_8\}$ by computing $M_6 = M_4 \oplus R_s$, $M_7 = h(M_{a2} \| M_5)$ and $M_8 = h(R_s)$ in the authentication phase.

*3.2. Server Masquerading Attack.* If the attacker can obtain the secret values $(e_i, r_i)$ from the user's smart card illegally by some means and intercept the message $\{M_2\}$ in the login phase and $\{M_6, M_7, M_8\}$ in the authentication phase, the attacker can perform the server masquerading attack as the following steps. The procedure of the server masquerading attack is illustrated in Figure 1.

(SA1) The attacker $A_i$ computes the following equations, where $R_{as}$ is a random number chosen by the attacker:

$$\begin{aligned} M_{a4} &= e_i \oplus r_i, \\ M_{a5} &= M_2 \oplus M_{a4}, \\ M_{a6} &= M_{a4} \oplus R_{as}, \\ M_{a7} &= h(M_2 \| M_{a5}), \\ M_{a8} &= h(R_{as}). \end{aligned} \tag{4}$$

(SA2) Then, $A_i$ sends the forged message $\{M_{a6}, M_{a7}, M_{a8}\}$ to the user $C_i$.

(SA3) Upon receiving the forged message, $C_i$ checks whether $M_{a7} = h(M_2 \| R_c)$ or not. If they are equal, $C_i$ computes $M_9 = M_{a6} \oplus M_1$.

(SA4) $C_i$ verifies whether $M_{a8} = h(M_9)$ or not. If it holds, $C_i$ will be convinced the message $\{M_{a6}, M_{a7}, M_{a8}\}$ sent from the legal server.

(SA5) Then, $C_i$ makes the reply massage $\{M_{10}\}$ by computing $M_{10} = h(M_{a6} \| M_9)$ in the authentication phase.

*3.3. Password Guessing Attack.* If an attacker can extract the secret values $(r_i, f_i)$ from the legal user's smart card by some means, the attacker can easily find out $PW_i$ by performing the password guessing attack, in which each guess $PW_i^*$ for $PW_i$ can be verified as the following steps.

(PA1) The attacker $A_i$ computes the secret parameter $r_i^* = h(PW_i^*) \oplus f_i$ from the registration phase.

(PA2) $A_i$ verifies the correctness of $PW_i^*$ by checking $r_i = r_i^*$.

(PA3) $A_i$ repeats the above steps until a correct password $PW_i^*$ is found.

Thus, the attacker can perform the password guessing attack, and can successfully impersonate the legal user with the guessed user password.

*3.4. Insider Attack.* In the registration phase, if the user's password $PW_i$ and biometrics information $B_i$ are revealed to the server, the insider of the server may directly obtain the user's password and biometrics information. Thus, the insider of the server as an attacker can impersonate as the legal user to access the user's other accounts in other server if the user uses the same password for the other accounts.

*3.5. Mutual Authentication.* Generally, if authentication scheme is insecure against user impersonation attack and server masquerading attack, the authentication schemes cannot provide mutual authentication between the user and the remote server. Therefore, Das's scheme fails to provide mutual authentication as described in Sections 3.1 and 3.2. Namely, if the attacker can obtain the secret values $(e_i, r_i)$ from the legal user's smart card by some means and intercept the messages communicating between the user and the server, the attacker can make the forged messages easily by computing $M_{a1} = e_i \oplus r_i$, $M_{a2} = M_{a1} \oplus R_{ac}$, and $M_{a3} = h(R_{ac})$ in the login phase. Also, the attacker can make the forged messages easily by computing $M_{a6} = M_{a4} \oplus R_{as}$, $M_{a7} = h(M_2 \| M_{a5})$, and $M_{a8} = h(R_{as})$ in the authentication phase.

## 4. The Enhanced Scheme

In this section, we propose an enhanced Das's scheme which not only can withstand the various attacks, but also provide mutual authentication between the user and the server. The enhanced scheme is divided into three phases: registration phase, login phase, and authentication phase.

*4.1. Registration Phase.* Before logging to the remote server $S_i$, a user $C_i$ initially has to register to the trusted registration centre $R_i$ as the following steps. The registration phase is illustrated in Figure 2.

(R1) $C_i$ submits his identity $ID_i$ and password information $(PW_i \oplus K)$ to $R_i$ through a secure channel. Also the user submits his biometrics information $(B_i \oplus K)$ via the specific device to $R_i$, where $K$ is a random number generated by $C_i$.

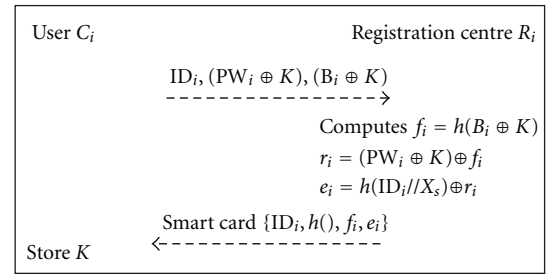


Figure 2: Registration phase of the enhanced scheme.

(R2) $R_i$ computes $f_i = h(B_i \oplus K)$, $r_i = h(PW_i \oplus K) \oplus f_i$ and $e_i = h(ID_i \| X_s) \oplus r_i$, where $X_s$ is a secret value generated by the server.

(R3) $R_i$ stores $(ID_i, h(), f_i, e_i)$ on the user's smart card and sends it to the user via a secure channel. And $C_i$ stores random number $K$ into the smart card issued by $R_i$.

*4.2. Login Phase.* When the user $C_i$ wants to login the remote server $S_i$, the user has to perform the following steps. The login phase and authentication phase are illustrated in Figure 3.

(L1) $C_i$ inserts his smart card into a card reader and inputs the biometrics information $B_i$ on the specific device to verify user's biometrics. If the biometrics information $h(B_i \oplus K)$ matches $f_i$ stored in the system, $C_i$ passes the biometrics verification.

(L2) $C_i$ inputs the $ID_i$ and $PW_i$, and then the smart card computes the following equations, where $R_c$ is a random number generated by the user:

$$\begin{aligned} r_i' &= h(PW_i \oplus K) \oplus f_i, \\ M_1 &= e_i \oplus r_i', \\ M_2 &= M_1 \oplus R_c, \\ M_3 &= h(M_1 \| R_c). \end{aligned} \tag{5}$$

(L3) $C_i$ sends the login request message $\{ID_i, M_2, M_3\}$ to $S_i$.

*4.3. Authentication Phase.* After receiving the request login message, the remote server $S_i$ has to perform the following steps with the user $C_i$ to authenticate each other.

(A1) $S_i$ checks the format of $ID_i$.

(A2) If the $ID_i$ is valid, $S_i$ computes $M_4 = h(ID_i \| X_s)$ and $M_5 = M_2 \oplus M_4$.

(A3) $S_i$ verifies whether $M_3 = h(M_4 \| M_5)$ or not. If they are equal, $S_i$ computes the following equations, where $R_s$ is a random number generated by the server:

$$\begin{aligned} M_6 &= M_4 \oplus R_s, \\ M_7 &= h(M_4 \| R_s). \end{aligned} \tag{6}$$

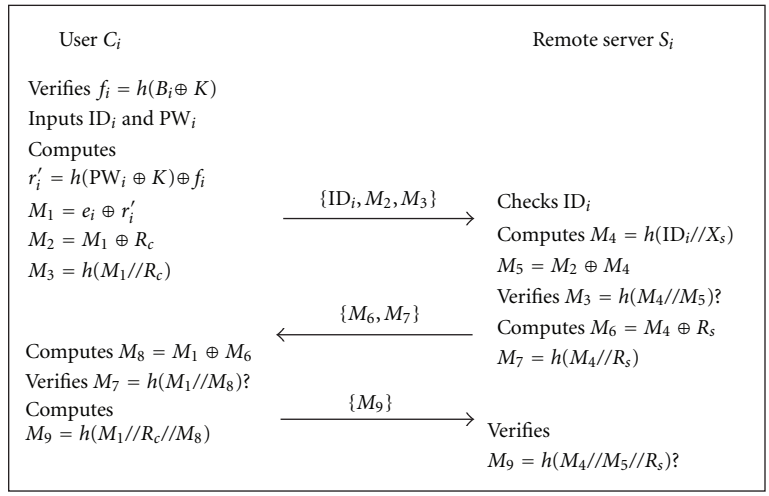


Figure 3: Login phase and authentication phase of the enhanced scheme.

(A4) Then, $S_i$ sends the message $\{M_6, M_7\}$ to $C_i$.

(A5) After receiving the reply message, $C_i$ computes $M_8 = M_6 \oplus M_1$ and verifies whether $M_7 = h(M_1 \| M_8)$ or not. If they are equal, $C_i$ computes $M_9 = h(M_1 \| R_c \| M_8)$.

(A6) Then, $C_i$ sends the message $\{M_9\}$ for authentication to $S_i$.

(A7) After receiving the message, $S_i$ verifies whether $M_9 = h(M_4 \| M_5 \| R_s)$ or not. If they are equal, $S_i$ accepts the user's login request.

## 5. Security Analysis of the Enhanced Scheme

In this scheme, we will provide the security analysis of the enhanced scheme based on the password and biometrics information. To analyze the security of the enhanced scheme, we assume that an attacker can access a user's smart card and extract the secret values stored in the smart card by some means [14, 15], and intercept the messages communicating between the user and the server.

*5.1. User Impersonation Attack.* To impersonate as the legitimate user, an attacker attempts to make a forged login request message which can be authenticated to the server. However, the attacker cannot impersonate as the legitimate user by forging the login request message even if the attacker can extract the secret values $(f_i, e_i)$ stored in the user's smart card, because the attacker cannot compute the login request message $(M_2, M_3)$ without knowing the secret value $X_s$ kept by the server. Hence, the attacker has no chance to login to the enhanced scheme by launching the user impersonation attack.

*5.2. Server Masquerading Attack.* To masquerade as the legitimate server, an attacker attempts to make the forged reply message which can be masqueraded to the user when receiving the user's login request message. However, the attacker cannot masquerade as the server by forging the reply message, because the attacker cannot compute $(M_6, M_7)$ sending to the user without knowing the secret value $X_s$ kept by the server. Hence, the attacker cannot masquerade as the legitimate server to the user by launching the server masquerading attack.

*5.3. Password Guessing Attack.* After the attacker extracts the secret values $(f_i, e_i, K)$ stored in the user's smart card under the described assumption, the attacker attempts to derive the user's password $PW_i$ using $r_i = h(PW_i \oplus K) \oplus f_i$ in the registration phase. However, the attacker cannot guess the user's password $PW_i$ using the secret values extracted from the legitimate user's smart card, because the attacker cannot compute the secret value $r_i$ without knowing the secret value $X_s$ kept by the server.

*5.4. Insider Attack.* In the registration phase, if the user's password $PW_i$ and the biometrics information $B_i$ are revealed to the server, the insider of the server may directly obtain $PW_i$ and $B_i$ and impersonate as the user to access user's other accounts in other server. But, the enhanced scheme is secure against the insider attack, because the user submits $h(PW_i \oplus K)$ instead of $PW_i$ and $h(B_i \oplus K)$ instead of $B_i$.

*5.5. Mutual Authentication.* As described in Sections 5.1 and 5.2, the enhanced scheme can withstand the user impersonation attack and the server masquerading attack, consequently the proposed scheme provides mutual authentication between the user and the remote server. Namely, even if the attacker can extract the secret values $(f_i, e_i)$ stored in the user's smart card, the user can be authenticated to the server and the server can be authenticated to the user. Because the attacker cannot make the login request message $\{ID_i, M_2, M_3\}$ and the reply message $\{M_6, M_7\}$ without knowing the secret value $X_s$ kept by the server.

Table 2: Security comparison of the related scheme and the enhanced scheme.

| Security features | Li-Hwang's scheme [12] | Das's scheme [13] | Enhanced scheme |
|---|---|---|---|
| User impersonation attack | Possible | Possible | Impossible |
| Sever masquerading attack | Possible | Possible | Impossible |
| Password guessing attack | Possible | Possible | Impossible |
| Insider attack | Possible | Possible | Impossible |
| Mutual authentication | Not provided | Not provided | Provided |

*5.6. Security Comparison of the Related Scheme and the Enhanced Scheme.* The security analysis of the related scheme and the enhanced scheme is summarized in Table 2. The enhanced scheme is relatively more secure than Li-Hwang's and Das's scheme. In addition, the enhanced scheme provides mutual authentication between the user and the server.

## 6. Conclusions

In this paper, we analyzed the security of Das's scheme. And we have shown that Das's scheme is not secure against the various attacks and fails to provide mutual authentication between the user and the server. Also, we proposed the enhanced scheme to overcome these security weaknesses, while preserving all their merits, even if the secret information stored in the smart card is revealed. As a result of security analysis, the enhanced scheme is secure against the user impersonation attack, the server masquerading attack, and the password guessing attack, the insider attack and provides mutual authentication between the user and the server.

## Acknowledgment

This work was supported by Kangnam University Research grant.

## References

[1] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[2] M. S. Hwang and 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.

[3] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, "Further improvement of an efficient password based remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 612–614, 2004.

[4] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 629–631, 2004.

[5] C. W. Lin, C. S. Tsai, and M. S. Hwang, "A new strong-password authentication scheme using one-way Hash functions," *Journal of Computer and Systems Sciences International*, vol. 45, no. 4, pp. 623–626, 2006.

[6] C. S. Bindu, P. Reddy, and B. Satyanarayana, "Improved remote user authentication scheme preserving user anonymity," *International Journal of Computer Science and Network Security*, vol. 83, pp. 62–66, 2008.

[7] W. C. Ku, S. T. Chang, and M. H. Chiang, "Further cryptanalysis of fingerprint-based remote user authentication scheme using smartcards," *Electronics Letters*, vol. 41, no. 5, pp. 240–241, 2005.

[8] M. K. Khan and J. Zhang, "An efficient and practical fingerprint-based remote user authentication scheme with smart cards," *Lecture Notes in Computer Science*, vol. 3903, pp. 260–268, 2006.

[9] A. Baig, A. Bouridane, F. Kurugollu, and G. Qu, "Fingerprint-Iris fusion based identification system using a single hamming distance matcher," *International Journal of Bio-Science and Bio-Technology*, vol. 1, no. 1, pp. 47–58, 2009.

[10] J. Pedraza, M. A. Patricio, A. de Asís, and J. M. Molina, "Privacy and legal requirements for developing biometric identification software in context-based applications," *International Journal of Bio-Science and Bio-Technology*, vol. 2, no. 1, pp. 13–24, 2010.

[11] C. C. Chang, S.C. Chang, and Y.W. Lai, "An improved biometrics-based user authentication scheme without concurrency system," *International Journal of Intelligent Information Processing*, vol. 1, no. 1, pp. 41–49, 2010.

[12] C. T. Li and M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 1–5, 2010.

[13] A. K. Das, "Analysis and Improvement on an efficient biometric-based remote user authentication scheme using smart cards," *IET Information Security*, vol. 5, no. 3, pp. 541–552, 2011.

[14] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," *Proceedings of Advances in Cryptology*, pp. 388–397, 1999.

[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*, vol. 51, no. 5, pp. 541–552, 2002.