International Journal of Internet, Broadcasting and Communication Vol.8 No.3 41-49 (2016)
http://dx.doi.org/10.7236/IJIBC.2016.8.3.41

IJIBC 16-3-5

A Strong Biometric-based Remote User Authentication Scheme for Telecare Medicine Information Systems with Session Key Agreement

Younghwa An

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

Abstract

Recently, many biometrics-based user authentication schemes for telecare medicine information systems (TMIS) have been proposed to improve the security problems in user authentication system. In 2014, Mishra et al. proposed an improvement of Awasthi-Srivastava's biometric based authentication for TMIS which is secure against the various attacks and provide mutual authentication, efficient password change. In this paper, we discuss the security of Mishra et al.'s authentication scheme, and we have shown that Mishra et al.'s authentication scheme is still insecure against the various attacks. Also, we proposed the improved scheme to remove these security problems of Mishra et al.'s authentication scheme, even if the secret information stored in the smart card is revealed. As a result, we can see that the improved biometric based authentication scheme is secure against the insider attack, the password guessing attack, the user impersonation attack, the server masquerading attack and provides mutual authentication between the user and the telecare system.

Keywords: *Authentication, Biometrics, Password, Telecare Medicine Information System*

1. Introduction

Telecare medicine information system (TMIS) provides certain healthcare services, which become a feasible solution to the continuously rising demand in medical and healthcare sector. Recently, with technological advances in mobile computing, the user authentication scheme in medical and healthcare sector 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 [2-6] have proposed the enhanced password-based authentication protocols to improve security problems. Also, lots of biometrics-based authentication protocols [7-11] have been proposed.

Generally, biometrics-based remote user authentication is inherently more secure and reliable than the

Manuscript Received: Jun. 15, 2016 / Revised: Jun. 23, 2016 / Accepted: Jul. 15, 2016

Corresponding Author: yhan@kangnam.ac.kr
Tel: +82-31-280-3756
Computer Media Information Engineering, Kangnam University

traditional authentication scheme, because biometrics keys have some of the following advantages as compared to traditional passwords.

- 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, Awasthi-Srivastava [10] proposed a biometric authentication scheme for telecare medicine information system with nonce. They claimed that their scheme not only resists the impersonation attack, the stolen smart card attack, the privileged insider attack etc. but also avoids the computation of time consuming exponential operation for low cost mobile devices. But Mishra et al. [11], in 2014, pointed out that Awasthi-Srivastava's scheme fails to resist online and off-line password guessing attack. Additionally, they showed that password change phase of Awasthi-Srivastava's scheme is inefficient to identify the correct input. Then, Mishra et al. proposed an improvement of Awasthi-Srivastava's biometric based authentication for TMIS which is secure against the insider attack, the user impersonation attack, the replay attack, the parallel session attack, the off-line password attack etc. and provide mutual authentication, efficient password change.

In this paper, we briefly discuss the security of Mishra et al.'s authentication scheme for TMIS and we have shown that Mishra et al.'s authentication scheme is still vulnerable to the various attacks and does not provide mutual authentication. Also, we propose the improved scheme to remove these security problems of Mishra et al.'s authentication scheme, even if the secret information stored in the mobile device (such as smart card) is revealed to an attacker. To analyze Mishra et al.'s authentication scheme, we assume that an attacker could obtain the secret values stored in the smart card by monitoring the power consumption [12-13] and intercept messages communicating between the user and the telecare system. Also, we assume that an attacker may possess the following capabilities to thwart the security schemes.

- 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.
- 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 Mishra et al.'s authentication scheme. In section 3, we describe the security analysis of Mishra et al.'s authentication scheme. The improved scheme is presented in section 4, and its security analysis of the improved scheme is given in section 5. Finally, conclusions are presented in section 6.

2. Reviews of Mishra 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	User/Patient
S	A trustworthy medical system
MD	Mobile device
ID_U	Unique identity of U
PW_U	Unique password of U
B_U	Personal biometrics of U
x	Master key of S
$h()$	A secure hash function
$H()$	Biohashing
$x \parallel y$	x concatenates with y
$x \oplus y$	XOR operation of x and y

2.1 Registration Phase

Before logging in the telecare medicine information system S, a user U initially has to register to the telecare system S as the following steps.

R1. U selects his identity ID_U and password PW_U, and chooses a random nonce N. Also the user imprints his biometrics B_U at the sensor.

R2. U computes $(PW_U \oplus N)$, $(H(B_U) \oplus N)$ and then submits the registration request information with ID_U, $(PW_U \oplus N)$, $(H(B_U) \oplus N)$ to S via secure channel.

R3. Upon receiving the registration request information, S computes $(PW_U \oplus N) \oplus (H(B_U) \oplus N) = PW_U \oplus H(B_U)$ and $A_U = h(ID_U \,//\, x \,//\, T_R)$, where T_R is the registration time. Also, S computes $X_U = h(A_U)$ and $V_U = A_U \oplus (PW_U \oplus H(B_U))$.

R4. S stores these personalized security parameters $\{ID_U, X_U, V_U, h(), H()\}$ in the user's mobile device.

2.2 Login Phase

When a user U wants to login the telecare system, U has to perform the following steps.

L1. U first initiates the application on the device and then inputs his password PW_U. Also U imprints his biometrics B_U at the sensor.

L2. Mobile device computes $A_U = V_U \oplus (PW_U \oplus H(B_U))$. If X_U equals $h(A_U)$, the mobile device computes the following equation, $D_U = h(A_U \,//\, T_U)$, where T_U is a current timestamp of the mobile device.

L3. Finally, U sends the login message $\{ID_U, D_U, T_U\}$ to the telecare system S.

2.3 Authentication Phase

After receiving the login message, the telecare system S has to perform the following steps with the user U to authenticate each other.

A1. S verifies the freshness of timestamp, $T'_U - T_U \leq \Delta T$, where ΔT is the valid time delay. If the condition holds, S computes $A_U = h(ID_U \parallel x \parallel T_R)$ and then verifies $D_U = ?h(A_U \parallel T_U)$. If verification holds, U is authenticated by S.

A2. S computes $D_S = h(D_U \parallel A_U \parallel T_S)$, then sends mutual authentication message $\{D_S, T_S\}$ to U at time T_S.

A3. Upon receiving the mutual authentication message, U verifies the freshness of timestamp, $T_S - T_U \leq \Delta T$, where ΔT is the valid time delay. If the condition holds, U verifies $D_S = ?h(D_U \parallel A_U \parallel T_S)$. If verification holds, S is authenticated by U.

3. Security Analysis of Mishra et al.' Scheme

In this section, we will analyze Mishra et al.'s scheme. To analyze the security weaknesses, we assume that an attacker could obtain the secret values stored in the mobile device (such as smart card) by monitoring the power consumption [12-13] and intercept messages communicating between the user and the telecare system. Under this assumption, we will show that Mishra et al.'s scheme is vulnerable to the various attacks, such as the insider attack, the off-line password guessing attack, the user impersonation attack, the server masquerading attack etc. and cannot provide mutual authentication between the user and the telecare system.

3.1 Insider Attack

A malicious insider in the telecare system may try to acquire user's secrets, such as the user's password and biometrics information. In the registration phase, since the user's password information ($PW_U \oplus N$) and biometrics information ($H(B_U) \oplus N$) are revealed to the telecare system, a malicious insider in the telecare system can obtain the user's security information ($PW_U \oplus H(B_U)$). Therefore, the malicious insider can perform the off-line password guessing attack and the user impersonation attack etc. with the user's security information.

3.2 Off-line Password Guessing Attack

If an attacker is a malicious insider in the telecare system, and can extract the secret values (X_U, V_U) illegally from the legal user's mobile device by some means[ ], the attacker can easily find out PW_U by performing the off-line password guessing attack, in which each guess PW'_U for PW_U can be verified by the following steps.

PA1. The attacker computes secret parameter $A_U = V_U \oplus (PW_U \oplus H(B_U))$ with the secret values (X_U, V_U) extracted.

PA2. The attacker verifies the correctness of PW'_U by checking $X_U =? h(A_U)$.

PA3. The attacker repeats the above steps until a correct password PW'_U is found.

3.3 User Impersonation Attack

With the security information ($PW_U \oplus H(B_U)$) as described in subsection 3.1 and the secret values (X_U, V_U) as described in subsection 3.2, the attacker can perform the user impersonation attack as the following steps.

UA1. The attacker computes the following equations.

$$A'_U = V_U \oplus (PW_U \oplus H(B_U))$$

$$D'_U = h(A'_U \| T_A)$$

where T_A is a current timestamp of the attacker in the login phase.

UA2. Then, the attacker sends the forged login message $\{ID_U, D'_U, T_A\}$ to S.

UA3. Upon receiving the forged login message, S verifies the freshness of timestamp, $T'_A - T_A \leq \Delta T$. If it holds, S computes $A_U = h(ID_U \| x \| T_R)$ and then verifies $D'_U =? h(A_U \| T_A)$. If verification holds, the attacker as the legitimate user is authenticated by S.

3.4 Server Masquerading Attack

If the attacker can obtain the secret information ($PW_U \oplus H(B_U)$) as described in subsection 3.1 and the secret value (V_U) as described in subsection 3.2, and if the attacker can intercept the secret value (D_U, T_U) in the login phase, the attacker can perform the server masquerading attack as the following steps.

SA1. The attacker computes the following equations.

$$D'_S = h(D_U \| A'_U \| T_A)$$

where T_A is a current timestamp of the attacker in the authentication phase.

A2. Then the attacker sends the mutual authentication message $\{D'_S, T_A\}$ to U at time T_A.

A3. Upon receiving the mutual authentication message, U verifies the freshness of timestamp, $T_A-T_U \leq \Delta T$, where ΔT is the valid time delay. If the condition holds, U verifies $D_S=?h(D_U \parallel A_U \parallel T_A)$. If verification holds, the attacker as the legitimate telecare system is authenticated by U.

3.5 Mutual Authentication

Generally, if authentication scheme is insecure against user impersonation attack, server masquerading attack as described in subsection 3.3, 3.4, the authentication schemes cannot provide mutual authentication between the user and the telecare system. Therefore, Mishra et al.'s scheme fails to provide mutual authentication.

4. The Improved Scheme

In this section, we propose a strong biometric-based remote User authentication scheme for telecare medicine information system (TMIS) that improved Mishra et al.'s scheme which cannot withstand the various attacks. The improved scheme is divided into three phases: registration phase, login phase and authentication phase.

In order to initialize the biometrics based authentication scheme, the user U selects large prime number p and q, and computes $n=p\cdot q$. Then, the user U chooses a prime e and an integer d, such that $e\cdot d \bmod (p-1)(q-1)=1$, where e is the user's public key, and d is the user's private key.

4.1 Registration Phase

Before logging in the telecare medicine information system S, a user U initially has to register to the telecare system S as the following steps. The registration phase is illustrated in figure 1.

R1. U selects his identity ID_U and password PW_U, and chooses a random nonce K. Also the user imprints his biometrics B_U at the sensor.

R2. U computes $h(PW_U \oplus K)$, $h(B_U \oplus K)$ and then submits the registration request information with ID_U, $h(PW_U \oplus K)$, $h(B_U \oplus K)$ to S via secure channel.

R3. Upon receiving the registration request information, S computes the following equations.

$$A_U=(h(PW_U \oplus K) \oplus h(B_U \oplus K))^e$$

$$B_U=(A_U \oplus h(ID_U \oplus x))^e$$

R4. S stores these personalized security parameters $\{ID_U, A_U, B_U, h()\}$ in the user's mobile device. And U stores random number K into the user's mobile device issued by S.

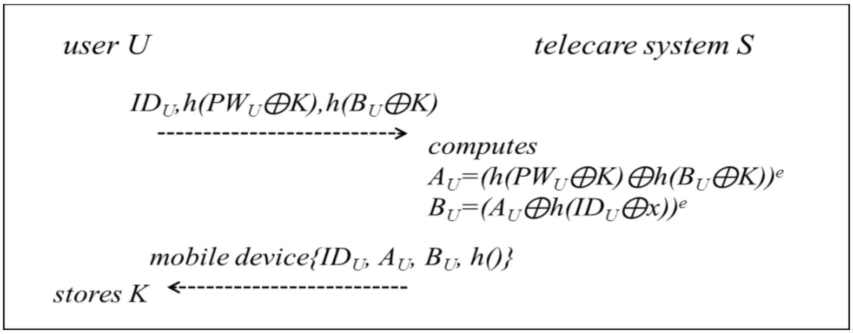

Figure1. Registration phase of the improved scheme

4.2 Login Phase

When the user U wants to login the telecare system, a user has to perform the following steps. The registration and authentication phase is illustrated in figure 2.

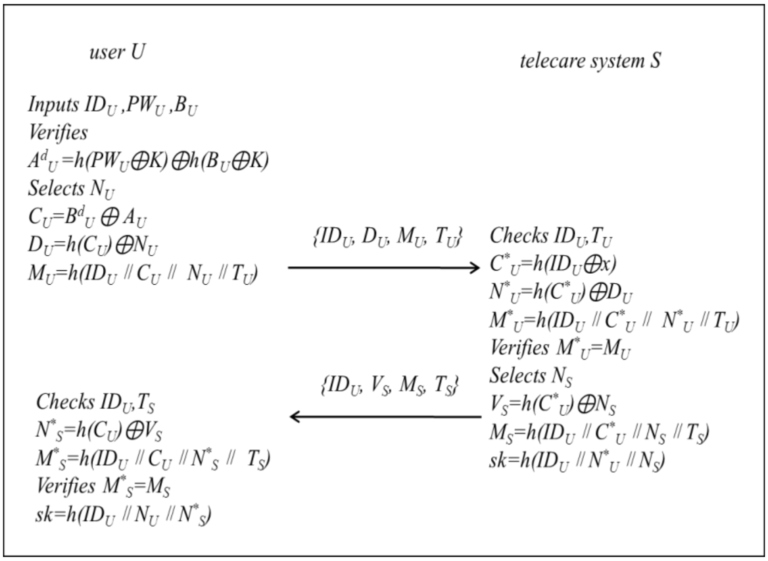
user U
telecare system S
Inputs ID_U ,PW_U ,B_U
Verifies
$A^d_U=h(PW_U\oplus K)\oplus h(B_U\oplus K)$
Selects N_U
$C_U=B^d_U \oplus A_U$
$D_U=h(C_U)\oplus N_U$
$M_U=h(ID_U \| C_U \| N_U \| T_U)$
$\{ID_U, D_U, M_U, T_U\}$
Checks ID_U,T_U
$C^*_U=h(ID_U\oplus x)$
$N^*_U=h(C^*_U)\oplus D_U$
$M^*_U=h(ID_U \| C^*_U \| N^*_U \| T_U)$
Verifies $M^*_U=M_U$
Selects N_S
$\{ID_U, V_S, M_S, T_S\}$
$V_S=h(C^*_U)\oplus N_S$
$M_S=h(ID_U \| C^*_U \| N_S \| T_S)$
$sk=h(ID_U \| N^*_U \| N_S)$
Checks ID_U,T_S
$N^*_S=h(C_U)\oplus V_S$
$M^*_S=h(ID_U \| C_U \| N^*_S \| T_S)$
Verifies $M^*_S=M_S$
$sk=h(ID_U \| N_U \| N^*_S)$

Figure2. Login phase and authentication phase of the improved scheme

L1. U first initiates the application on the device and then inputs his password PW_U. Also the user imprints his biometrics B_U at the sensor.

L2. Mobile device computes $(h(PW_U\oplus K)\oplus h(B_U\oplus K))$ and then verifies whether the computed value equals A^d_U or not. If the verification holds, the mobile device computes the following equation. Otherwise, it terminates the session.

$$C_U=B^d_U\oplus A_U$$

$$D_U=h(C_U)\oplus N_U$$

$$M_U=h(ID_U \| C_U \| N_U \| T_U)$$

where N_U is a random number generated by U and T_U is a current timestamp of the mobile device.

L3. Finally, U sends the login message $\{ID_U, D_U, M_U, T_U\}$ to the telecare system S.

4.3 Authentication Phase

After receiving the login message, the telecare system S has to perform the following steps with the user U to authenticate each other.

A1. S verifies the freshness of timestamp, $T^{'}_U-T_U\leq\Delta T$, where ΔT is the valid time delay. If the condition holds, the telecare system S computes $C^*_U=h(ID_U\oplus x)$, $N^*_U=h(C^*_U)\oplus D_U$, and then verifies whether M_U equals $h(ID_U \| C^*_U \| N^*_U \| T_U)$ or not. If verification holds, U is authenticated by S.

A2. Then, S computes the following equation.

$$V_S= h(C^*_U)\oplus N_S$$

$$M_S=h(ID_U \| C^*_U \| N_S \| T_S)$$

$$sk=h(ID_U \| N^*_U \| N_S)$$

where N_S is a random number generated by S and T_S is a current timestamp of the telecare system.

A3. Then S sends the mutual authentication message $\{ID_U, V_S, M_S, T_S\}$ to U.

A4. Upon receiving the mutual authentication message, U verifies the freshness of timestamp, T_S-$T_U \leq \Delta T$, where ΔT is the valid time delay. If the condition holds, U computes $N^*_S=h(C_U)\oplus V_S$, and then verifies whether M_S equals $h(ID_U \| C_U \| N^*_S \| T_S)$ or not. If verification holds, S is authenticated by U.

A5. After achieving the mutual authentication, U also computes the session key $sk=h(ID_U \| N_U \| N^*_S)$. Therefore, they can use the session key sk for secrecy communication.

5. Security Analysis of the Improved Scheme

In this section, we will provide the security analysis of the improved biometrics based remote user authentication scheme for the telecare medicine information systems (TMIS).To analyze the improved scheme, we assume that an attacker as the insider could obtain the secret values stored in the mobile device (such as smart card) by monitoring the power consumption [12-13] and intercept messages communicating between the user and the telecare system.

5.1 Insider Attack

In the registration phase, if user's password PW_U and biometrics information B_U are revealed to telecare system, an attacker as the malicious insider may directly obtain PW_U, B_U and then the attacker can perform the user impersonation attack. But, the malicious insider has no way to get the secret information, because a user submits $h(PW_U\oplus K)$ instead of PW_U and $h(B_U\oplus K)$ instead of B_U. Therefore the improved scheme can resist the insider attack.

5.2 Off-line Password Guessing Attack

After the attacker as malicious insider in the telecare system extract the secret values (A_U, B_U) illegally from the legal user's mobile device by some means, the attacker attempts to derive the user's password PW_U using $A_U=(h(PW_U\oplus K)\oplus h(B_U\oplus K))^e$ in the registration phase. However, the attacker cannot guess the user's password PW_U using the secret values extracted from the legitimate user's mobile device, because the attacker cannot compute the secret values without knowing the secret encryption key d kept by the user.

5.3 Off-line Password Guessing Attack

To impersonate as the legitimate user, an attacker attempts to make a forged login message which can be authenticated to the server. However, the attacker cannot impersonate as the legitimate user by forging the login massage even if the attacker can extract the secret values (A_U, B_U) stored in the legal user's mobile device, because the attacker cannot compute the login message (D_U, M_U) sending to the telecare system without knowing the secret value x kept by the telecare system and the secret encryption key d kept by the user. Hence, the attacker has no chance to login to the improved authentication scheme by launching the user impersonation attack.

5.4 Server Masquerading Attack

To masquerade as the legitimate telecare system, an attacker attempts to make the forged mutual authentication message when receiving the user's login request message. However, the attacker cannot masquerade as the telecare system by forging the mutual authentication massage, because the attacker cannot compute (V_S, M_S) without knowing the secret value x kept by the telecare system. Hence, the attacker cannot masquerade as the legitimate telecare system to the user by launching the server masquerading attack.

5.5 Mutual Authentication

As described in subsection 5.3 and 5.4, because the improved scheme can withstand to the user impersonation attack and the server masquerading attack, we can say that the improved scheme provides mutual authentication between the user and the telecare system. Namely, even if an attacker can extract the secret values (A_U, B_U) stored in a user's mobile device, the improved scheme can perform the mutual authentication. In addition, after achieving the mutual authentication, the user and the telecare system can compute the shared session key $sk=h(ID_U || N_U || N_S)$ each other for secrecy communication.

5.6 Functionality Comparisons between the Related Scheme and the Improved Scheme

The functionality comparisons between the related scheme and the improved scheme are summarized in Table 2. As a result, the improved scheme is relatively more secure than the related schemes. In addition, the improved scheme provides mutual authentication between the user and the telecare system.

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

security features	Awasthi-Srivastsva's scheme [10]	Mishra's scheme [11]	Improved scheme
insider attack	impossible	possible	impossible
password guessing attack	possible	possible	impossible
user impersonation attack	possible	possible	impossible
sever masquerading attack	possible	possible	impossible
mutual authentication	not provided	not provided	provided

6. Conclusions

In this paper, we have shown that Mishra's scheme is not secure against the various attacks, such as the insider attack, the off-line password guessing attack, the user impersonation attack, the sever masquerading attack and fails to provide mutual authentication between the user and the telecare system. Also, we proposed the improved scheme to overcome these various attacks, while preserving all their merits, even if the secret information stored in the smart card is revealed. As a result, the improved scheme is relatively more secure than the related schemes.

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] M.S. Hwang and L.H. Li, "A New Remote User Authentication Scheme Using Smart Cards," IEEE Transactions on Consumer Electronics, vol. 46, pp. 28-30, 2000.

[3] M.L. Das, A. Sxena and V.P. Gulathi, "A Dynamic ID-based Remote User Authentication Scheme," IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 629-631, 2004.

[4] 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.

[5] R.J. Robies and T.H. Kim," Applying Asymmetric Key Encryption to Secure Internet based SCADA," The International Journal of Internet, Broadcasting and Communication (IJIBC), vol. 4, no. 2, pp. 17-21, 2012.

[6] 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.

[7] 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.

[8] 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, pp. 1-5, 2010.

[9] A.K. Das, "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.

[10] A.K. Awasthi, K. Srivastava, "A Biometrics Authentication Scheme for Telecare Medicine Information Systems with Nonce," Journal of Medicine Systems, vol. 37(5), pp. 1-4, 2013.

[11] D. Mishra, S. Mukhopadhyay, S. Kumar, M.K. Kyan, A.Chaturvedi, "Security Enhancement of a Biometric based Authentication Scheme for Telecare Medicine Information Systems with Nonce," Journal of Medicine Systems, vol. 38(41), pp. 1-11, 2014.

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

[13] 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.