On the Security of Yoon and Yoo's Biometrics Remote User Authentication Scheme

MING LIU *
Department of Tourism Management
WEN-GONG SHIEH
Department of Information Management
Chinese Culture University
No. 55, Hwa-Kang Road, Yang-Ming Shan, Taipei 11114
Taiwan, R.O.C.
lm2@faculty.pccu.edu.tw wgshieh@faculty.pccu.edu.tw

Abstract: - With the prevalence of electronic and mobile commerce, remote user authentication has become an essential component in identifying the legality of the log in user. Recently, Yoon and Yoo criticized the biometric-base authentication system proposed by Khan and Zhang that it is doubtful to parallel session attack and privileged insider's attack. Yoon and Yoo therefore proposed an improved scheme to correct Khan-Zhang's scheme. In addition, Yoon-Yoo's scheme largely reduced the computation cost of Khan-Zhang's scheme. In this paper, we demonstrate that the Yoon-Yoo's scheme is still vulnerable to offline password guessing attack to break the protocol. First, storing the fingerprint template in the smart card for fingerprint verification is not a good idea in Yoon-Yoo's scheme. Considering when the contents of the smart card are obtained by an adversary. Second, with the value from the previous valid login message, it allows the adversary to perform offline password guessing attack using the equation. Our study further proposed a secure improvement of Yoon-Yoo's scheme to correct the aforementioned security flaws with minimum alteration in the computation cost.

Key-Words: - Authentication, Cryptography, Impersonation attack, Password guessing attack, Security, Smart card

1 Introduction

In recent years, technology development has upgraded many industries and expanded the scope of services. Although hotels and restaurants are adapting to technology at a slower pace than other organizations, recent advancement shows more reliance on electronic and mobile commerce [1]. For example, La Quinta Inn and Suites, Omni Hotels, Choice Hotels International, and Starwood Hotels and Resorts have all developed mobile applications allowing customers to book rooms and access customer loyalty programs as well as other property-specific information [2]. With the prevalence of electronic and mobile commerce, remote user authentication has become an essential component in identifying the legality of the login user to a remote system. Smart card with its processing power and local memory is widely adopted in the applications of electronic and mobile commerce for secure transaction. In addition, smart card and password-based authentication schemes have been proposed as two factor security for user authentication [3-17]. However, to enhance the security problems caused by lose of smart card and weak user password, biometric-based authentication schemes with smart card are also well developed [18-26].

In 2012, Yoon and Yoo [27] criticized the biometric-base authentication system proposed by Khan and Zhang [24] and proposed an improved biometrics remote user authentication scheme. Yoon and Yoo demonstrate that Khan-Zhang's scheme is vulnerable to the following attacks:

1. It is doubtful to parallel session attack in which an opponent without knowing a legal user's password and biometrics information can deceive as the legal user by constructing a valid login message from eavesdropped communications between the user and the remote system;

2. It is insecure to privileged insider's attack since a legal user's password can be easily exposed to the insider attacker of the remote system.

Yoon and Yoo therefore proposed an improved scheme with more efficiency and stronger security. However, in this paper, we figure out that the Yoon-Yoo's scheme is still vulnerable to the offline password guessing attack. Moreover, we figure out a way to eliminate the security vulnerability of Yoon-Yoo's scheme. Compare to the Yoon-Yoo's scheme, our proposed scheme is more secured without raising much computation cost.

The rest of the paper is organized as follows. In section 2, we review Yoon-Yoo's authentication scheme. Next, in Section 3, we exhibit that Yoon and Yoo's scheme is vulnerable to offline guessing attack and impersonation attack. Then, we discuss the reasons behind the attacks in section 4. After that, we propose an improvement in section 5. Security and Efficiency analysis are presented in sections 6 and 7. Finally, we conclude the paper in the last section.

2 Review of Yoon and Yoo's biometrics remote user authentication scheme.

In this section, we review Yoon-Yoo's authentication scheme. There are three features with this protocol:

1. It is designed to significantly reduce the computation cost of each participant by using a small communication round.

2. It achieves cryptographic goals by employing lightweight operators, such as bit-wise exclusive-OR (XOR) operators and collision-free one-way hash functions as main cryptographic operations without using server's public key and digital signatures to achieve a low cost computation.

3. It prevents most well-known cryptographic attacks.

To prevent the parallel session attack in Khan–Zhang's scheme, Yoon-Yoo's scheme modifies the format of C_1 and C_2 transmitted during the login and authentication phases such that they are created with different structures. To prevent the proposed privileged insider attack, the proposed scheme uses a random nonce n to protect the password PW_i *in* the registration phase. There are four phases in the proposed schemes including registration, login, authentication, and password change. Abbreviations used in this paper are as follows:

- U_i: A user.
- ID_i : Public identity of U_i .
- PW_i : Secret and possibly weak password of U_i .
- S_i : Fingerprint template of U_i .
- X_s: Strong secret key of the remote system.
- T , T',T'', T''': Timestamps.
- ΔT : Expected valid time interval for transmission delay.
- $h(\cdot)$: Strong collision-resistant one-way hash function such as SHA-256.
- $\oplus$: Bit-wise XOR operation.

2.1 Registration phase

If a new user U_i desires to register with the remote server, he/she selects identity ID_i, password PW_i, and a random nonce n. Then, the user U_i imprints personally his/her fingerprint on the sensor. ID_i , $PW_i \oplus n$, and fingerprint are then send to the server through a secure channel. After receiving the registration request from U_i, the remote system of the registration center processes the following operations:

1. Generate fingerprint template S_i and calculate

$$PW_i' = h(PW_i \oplus n||S_i) \quad (1)$$

where $h(\cdot)$ represents collision-free one way hash function.

2. Calculate

$$Y_i = h(ID_i||X_S) \oplus PW_i' \quad (2)$$

where X_s is the secrete key of the registration server.

3. Release a smart card to the user over a secure channel which contains $h(\cdot)$, Y_i, S_i and ID_i .

After getting the smartcard from remote system, the user U_i enters n into his/her smartcard. Detailed registration phase is illustrated in Figure 1.

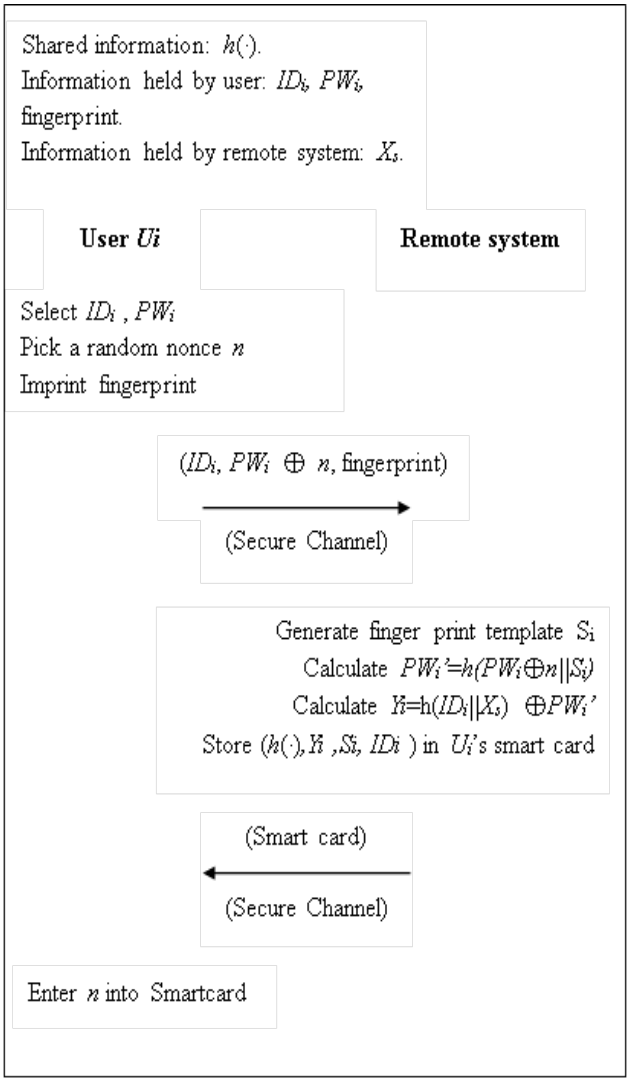

Fig. 1. Registration phase of Yoon and Yoo's scheme

2.2 Login phase

To login, the user U_i inserts his/her smart card into the reader of a terminal. He/she then imprints his/her fingerprint on the sensor to get S_i and keys in his/her password PW_i. If U_i passes the fingerprint verification by checking S_i, the smart card processes the following operations:

1. Calculate

$$PW_i" = h(PW_i \oplus n||S_i) \quad (3)$$

and

$$Y_i' = Y_i \oplus PW_i" = h(I D_i ||X_S). \quad (4)$$

2. Calculate

$$C_1 = h(Yi' ||T) \quad (5)$$

where T is the current timestamp of the login device.

3. Send login message $C = (IDi, C_1, T)$ to the remote system for authentication.

2.3 Authentication phase

When receiving the login message from the user at time T' the remote system processes the following operations:

1. Inspect whether the format of ID_i is correct or not. Discard the login request if it is not correct.

2. Validate if

$$(T' - T) \geq \Delta T \quad (6)$$

where ΔT is the valid time interval for transmission delay. If yes, the system discards the login request.

3. Check whether

$$C_1 = h(h(IDi ||X_S) ||T) \quad (7)$$

holds. If yes, the system accepts the user login, otherwise the login request is rejected.

4. Obtain the current timestamp $T"$.

5. Calculate

$$C_2 = h(C_1||h(ID_i ||X_S) ||T") \quad (8)$$

for mutual authentication.

6. Send message (C_2, $T"$) to U_i.

Upon obtaining the message (C_2, $T"$) at time T''', the smart card runs the following operations:

1. Stop the login procedure if $(T''' - T'') \geq \Delta T$.

2. Accept the responding party as the authentic system if

$$C_2 = h(C_1||Y_i'||T") \quad (9)$$

and the mutual authentication between *Ui* and the remote system is done. Otherwise, U_i ends the connection.

Detailed Login and authentication phase is illustrated in Figure 2.

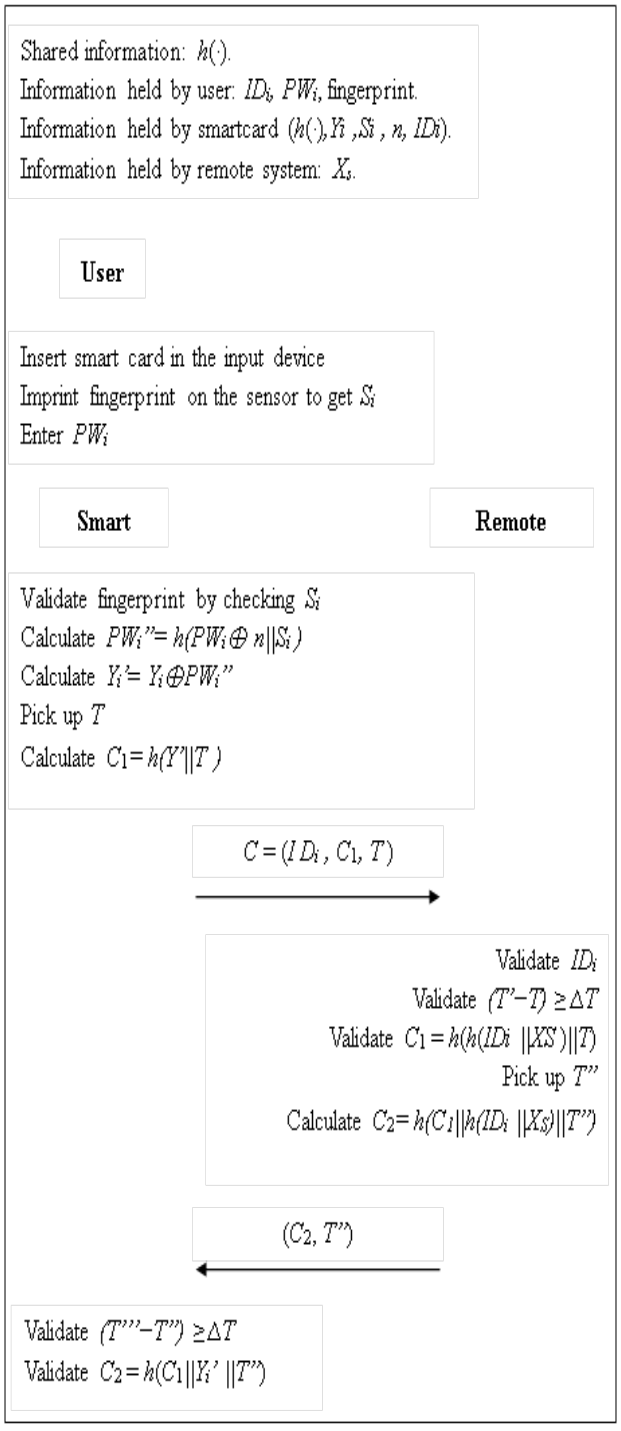

Fig. 2. Login and authentication phase of Yoon and Yoo's scheme

2.4 Password change phage

Whenever the user U_i requests to change his/her old password PW_i to a new password PW_i^*, U_i has to imprint his/her fingerprint to get the template S_i, then the smart card matches it with the stored template in the smart card. If they are equal, U_i enters the old password PW_i *and* the new password PW_i^*.

The client device then processes the following operations:

1. Calculate

$$PW_i" = h\,(PW_i \oplus n||S_i)$$
(10)

$$Y_i' = Y_i \oplus PW_i" = h\,(I\,Di\,||XS)$$
(11)

and

$$Y_i^* = Yi' \oplus h\,(PW_i^* \oplus n||S_i).$$
(12)

2. Substitute the old Y_i with the new Y_i^* in the smart card.

3 Security weakness of Yoon-Yoo's Scheme

This section shows that Yoon-Yoo's scheme is vulnerable to the following attacks.

3.1 Offline password guessing attack

An offline password guessing attack involves an adversary continuously trying, randomly or systematically, guessed user passwords, one at a time, without connecting the target remote system, in the hope of finding the correct user password of the remote system to break into the system using the user's account and password. Ensuring long-term passwords chosen from a large space can reduce such exhaustive searches. Most users, however, select passwords from a small subset of the full password space with respect to personal information, such as a birthday, a telephone number, and so on. Such passwords are called weak passwords, and can easily be guessed successfully by using the so-called offline password guessing attack. It is also called a dictionary attack where the passwords used in the guessing attack belong to a

weak password dictionary which is a small subset of the full password space with respect to personal information.

To successfully perform an offline password guessing attack to Yoon-Yoo's scheme, three factors must be available:

1. an existing weak user password of the system,
2. a high possibility of repeating guessing without the notice of the remote system, and
3. a comparison target for the adversary to verify the correctness of the guessed password.

Assume that an adversary has obtained the contents ($h(\cdot)$, Yi, Si, n, IDi) of a user smart card and the contents of the preciously intercepted old login message (IDi, C_1, T) of the user. We describe the repeating procedure of our offline password guessing to Yoon-Yoo's Scheme in the following algorithm:

Algorithm: Offline password guessing attack.

Input: A weak password dictionary with respect to the personal information of U_i, the contents ($h(\cdot)$,Y_i , S_i, n, ID_i) of the user smart card of U_i, and the contents (ID_i, C_1, T) of a previous valid login message of the user U_i at time T.

Step 1: If the weak password dictionary is not empty, select a password PW_i form the dictionary and remove the password PW_i from the dictionary. Otherwise, stop and output a failure message.

Step 2: Compute

$$PW_i" = h(PW_i \oplus n || S_i) \quad (13)$$

$$Y_i' = Y_i \oplus PW_i" \quad (14)$$

And

$$C_1' = h(Y_i' || T). \quad (15)$$

Step 3: If

$$C_1' = C_1 \quad (16)$$

output PW_i and stop successfully.
Otherwise, go back to Step 1.

Now, we show that our offline password guessing attack to Yoon-Yoo's scheme satisfies the above three factors. First of all, if the above algorithm stops at step 1 with a failure message output, it implies that the user uses a strong password, instead of a weak one in the weak password dictionary. Therefore, an existing weak user password of the system is required to successfully perform the guessing attack. Next, since our algorithm is performed locally without participation of the remote system, it can perform repeating guessing without the notice of the remote system. Finally, the C_1 value, in the previous valid login message (ID_i, C_1, T) of the user U_i at time T, is the comparison target for the adversary to verify the correctness of the guessed password as shown in step 3.

3.2 Impersonation attack using lost or stolen smartcards

An impersonation attack using lost or stolen smartcards means that when legal users lose their smart cards to an adversary or an adversary steals a smartcard of a legal user for a short duration and makes a duplicate of it, the adversary can masquerade as the legal user, using the information stored in the smart card, to login successfully into the remote system. Malicious parties may catch information stored in the smartcard of some user by some ways, such as obtaining the information in smartcard via illegal card readers.

With the information stored in smartcards of the user U_i, and messages intercepted during previous login transactions between the user and the remote system, we describe our impersonation attack algorithm as follows.

Algorithm: Impersonation attack using lost or stolen smartcards.

Input: A weak password dictionary with respect to the personal information of U_i, the contents ($h(\cdot)$,Y_i , S_i, n, ID_i) of the lost or stolen smartcard of U_i, and the contents (IDi, C_1, T) of a previous valid login message of the user U_i at time T.

Step 1: Perform the above offline password guessing attack to obtain the correct password PW_i of the user U_i. Stop if the password guessing attack fails with a failure message output. Otherwise, go to step 2.

Step 2: Compute

$$PW_i" = h(PW_i \oplus n || S_i) \quad (17)$$

$$Y_i' = Y_i \oplus PW_i" \quad (18)$$

and

$$C_1' = h(Y_i' || T') \quad (19)$$

where T' is the current timestamp of the adversary.

Step 3: Send the login message (ID_i, C_1', T') to the remote system.

As shown in the above algorithm, once the correct user password PW_i is obtained by the offline password guessing attack, the correct login message (ID_i, C_1', T') can easily be computed using PW_i, the contents $(h(\cdot), Y_i, S_i, n, ID_i)$ of the lost or stolen smartcard of U_i, and the current timestamp T' of the adversary. After receiving the login message, the remote system will accept the login request and see the adversary as the legal user U_i.

4 Reasons behind our successful attacks

This section provides briefly the reasons why our attacks can be performed successfully. First, storing the fingerprint template S_i in the smart card for fingerprint verification is not a good idea in Yoon-Yoo's scheme, considering when the contents $(h(\cdot), Yi, S_i, n, ID_i)$ of the smart card are obtained by an adversary. Note that the smart card will calculate $PW_i" = h(PW_i \oplus n||S_i)$ after the user passes the fingerprint verification in Yoon-Yoo's scheme. Storing S_i in the smart card will help the adversary in the computation of $PW_i"$. If the user password PW_i is also known to the adversary, all the information needed to compute $PW_i"$, including PW_i, n, and S_i will be available to the adversary. A possible improvement can store $h(S_i)$, instead of S_i, in the smart card for fingerprint verification, as shown in our proposed improvement in the next section.

Secondly, the value C_1, in the previous valid login message (ID_i, C_1, T) of the user U_i at time T, becomes the comparison target for the adversary to verify the correctness of the guessed password, if S_i is stored in the smart card. The adversary will find that $C_1 = h(Y_i'||T) = h(Y_i \oplus PW_i"||T) = h(Y_i \oplus h(PW_i \oplus n||S_i)||T)$. Note that, in the equation $C_1 = h(Y_i \oplus h(PW_i \oplus n||S_i)||T)$, PW_i is the only unknown value. The values C_1 and T in the equation can be found in the intercepted valid login message (ID_i, C_1, T). The values Y_i, n, and S_i in the equation can be obtained in the smart card. This is the critical weakness in Yoon-Yoo's scheme. It allows the adversary to perform offline password guessing attack using the equation. That is, the correct password PW_i of the user U_i will make the equation $C_1 = h(Y_i \oplus h(PW_i \oplus n||S_i)||T)$ hold true. The adversary then can decide if the guessed password PW_i is correct or not.

5 Proposed Authentication Scheme

This section introduces a secure improvement of Yoon-Yoo's scheme to correct the security flaws described in Section 3 with minimum alteration in the computation cost. To avert the aforementioned attacks, the proposed scheme adds the calculation of

$$h(S_i) \quad (20)$$

in the registration phase to avoid the storing of S_i in the smart card. Instead, $h(S_i)$ is stored in the smart card. There are four stages in the proposed schemes including registration, login, authentication, and password change like Yoon-Yoo's scheme. However, only the major altered contents are highlighted, including registration, login and authentication phases, and password change phase.

5.1 Proposed registration phase

The proposed scheme adds the calculation of $h(S_i)$ in the registration phase to avoid the storing of S_i in the smart card. Instead, $h(S_i)$ is stored in the smart card for fingerprint verification. A smart card is later issued to the user which contains $h(\cdot)$, Y_i, $h(S_i)$, and ID_i. Figure 3 shows the registration phase of the proposed scheme.

5.2 Proposed login phase and authentication phase

Figure 4 shows the login and authentication phase of our proposed scheme. With the replacement of storing $h(S_i)$ in the smart card for fingerprint verification instead of storing S_i in the registration phase, the computation of PW_i" from S_i by the attacker later in the login and authentication phase is then prevented. Secondly, the C_1 value is further secured from PW_i guessing attack in the login phase because the fingerprint template S_i is not available to the adversary.

Note that, compared with Yoon-Yoo's scheme, one more hash computation, $h(S_i)$, is performed by the smart card during the login phase. In our scheme,

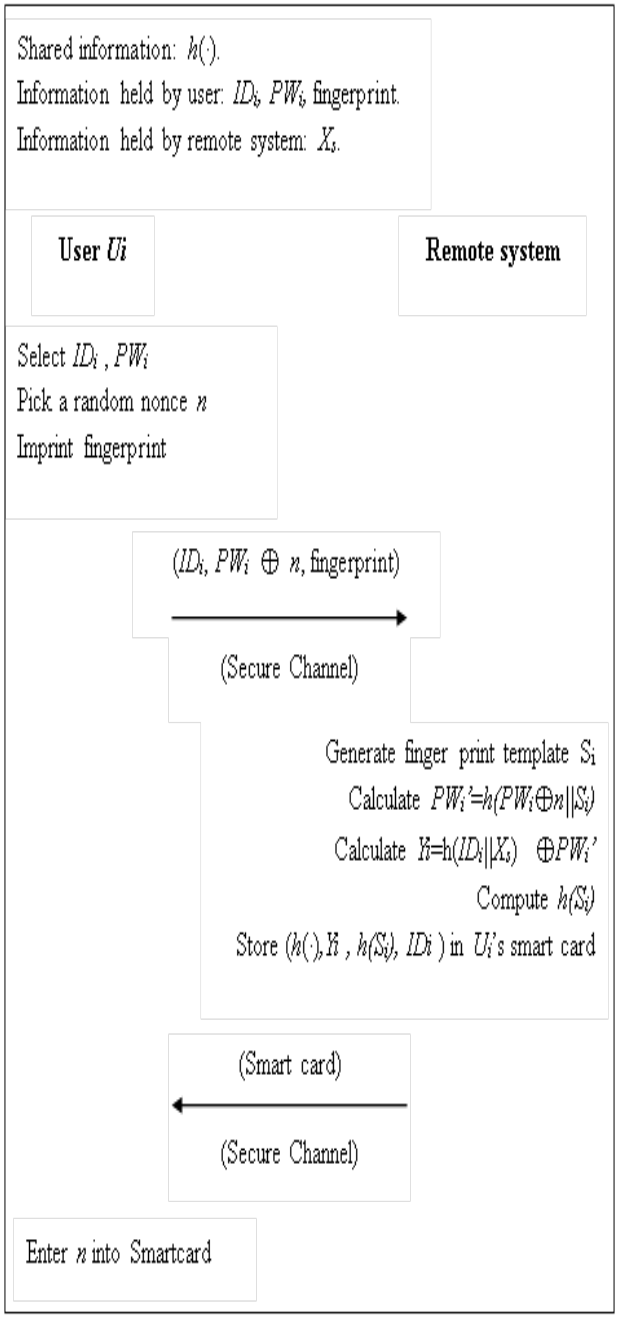

Fig 3. Proposed registration phase

instead of checking directly the fingerprint template S_i, the smart card compares the computed $h(S_i)$ with the stored $h(S_i)$. After that, the fingerprint template S_i, created immediately after the user imprints her/his fingerprint, is still needed in the following computation of

$$PW_i" = h\,(PW_i \oplus n||S_i\,) \quad (21)$$

in the smart card. It is how the user fingerprint plays its critical role in our proposed biometric-based

authentication scheme. That is, the fingerprint template S_i is not available to the adversary, not stored, and can only be created by the user at each login time.

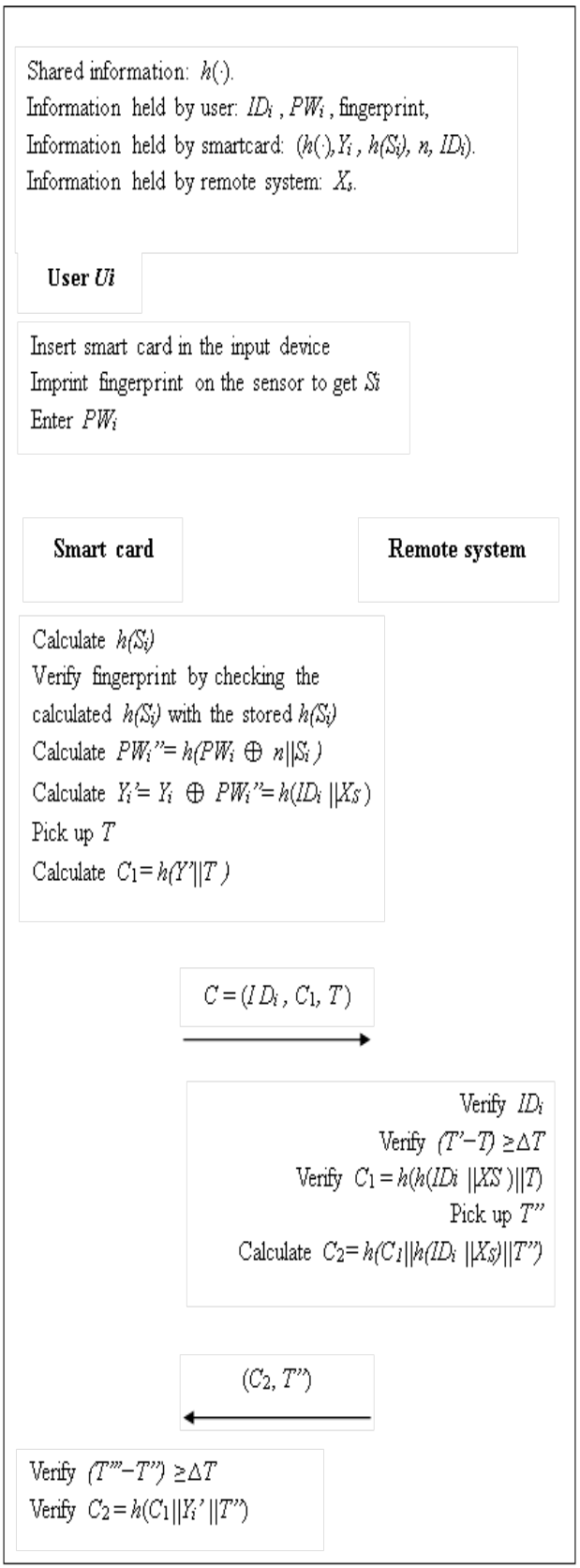

Fig. 4. Proposed Login and authentication phase

5.3 Proposed password change phage

Whenever U_i requests to change the old password PW_i to the new password PW_i^*, he/she has to imprint his/her fingerprint to get S_i. The smart card then calculate $h(S_i)$ to verify it with the stored $h(S_i)$.

If *Ui* passes the fingerprint validation, he/she enters the old password PW_i *and* the new password PW_i^*. The client device processes the following operations:

1. Calculate $PWi'' = h(PWi \oplus n||Si)$ (22)
2. Obtain the secret value *Yi'* as follows:

   $Yi' = Yi \oplus PWi'' = h(IDi||XS)$ (23)
3. Calculate a new *Yi** as follows:

   $Yi^* = Yi' \oplus h(PWi^* \oplus n||Si)$ (24)
4. Substitute the old *Yi* with the new *Yi* * on the smart card.

6 Security analysis

The security properties of Yoon-Yoo's scheme and that of the proposed scheme are summarized in Table 1. Based on the above described cryptanalysis of Yoon and Yoo's scheme, it is insecure to the guessing attack and the impersonation attack. Therefore, we can see that the proposed scheme is more secure in comparison to Yoon and Yoo's scheme.

	Yoon and Yoo's	Proposed Scheme
Replay attack	Secure	Secure
Guessing attack	Insecure	Secure
Parallel session attack	Secure	Secure
Reflection attack	Secure	Secure
Insider attack	Secure	Secure
Impersonation attack	Insecure	Secure
Mutual authentication	Insecure	Provided

Password change	Secure	Secure

Table 1. A comparison of security properties

7 Efficiency analysis

A comparison between the Yoon and Yoo's scheme and the proposed scheme is shown in Table 2. In addition to eliminating the security vulnerability of Yoon-Yoo's scheme, our proposed scheme does not increase much computation cost. The notation T_h is termed as the time for calculating the one-way hash function and the notation, and T_{xor} is termed as the time for calculating the bit-wise exclusive-or (XOR) operation.

In the registration phases, Yoon-Yoo's scheme needs a total of two hashing operation and two XOR operations; and the proposed scheme needs a total of three hashing operation and two XOR operations. In the login phase, Yoon-Yoo's scheme requires a total of two hashing operation and two XOR operations, and the proposed scheme requires a total of three hashing operation and two XOR operations. In the authentication and the password change phase, both the Yoon-Yoo's scheme and the proposed scheme requires four hashing operation. In the password change phase, both Yoon-Yoo's scheme and the proposed scheme requires two hashing operation and four XOR operations. The communication cost of both schemes is about 560 bits. While our proposed scheme holds the same communication cost of the Yoon-Yoo's scheme, the guessing attack and the impersonation attack are prevented.

	Yoon and Yoo's Scheme	Proposed Scheme
Registration phase	$2T_h + 2T_{xor}$	$3T_h + 2T_{xor}$
Login phase	$2T_h + 2T_{xor}$	$3T_h + 2T_{xor}$
Authentication phase	$4\ T_h$	$4\ T_h$
Password change phase	$2T_h + 4T_{xor}$	$3T_h + 4T_{xor}$
Communication cost	≈560 bits	≈560 bits

Table 2. A comparison of computation cost

8 Conclusion

Yoon-Yoo's (2012) authentication scheme not only improved the security of the biometric-base authentication system proposed by Khan and Zhang, it largely reduced the communication cost from 2448 bits to 560 bits. In this paper, we demonstrate that the Yoon-Yoo's scheme is still vulnerable to offline password guessing attack and impersonation attack using lost or stolen smartcards. Our study further figures out a way to eliminate the security vulnerability of Yoon-Yoo's scheme with minimum increase in the computation cost.

References:

[1] C. Muller, Hospitality technology: a review and reflection, *Hospitality Technology*, Vol.2, No.1, 2010, pp.9-19.

[2] G. R. Collins, Usable mobile ambient intelligent solutions for hospitality customers, *Journal of Information Technology Impact*, Vol.10, No.1, 2010, pp.45-54.

[3] T.-H. Chen, An authentication protocol with billing non-repudiation to personal communication systems, *International Journal of Innovative Computing, Information and Control*, Vol.5, No.9, 2009, pp.2657-2664.

[4] C.-T. Li, C.-H. Wei and Y.-H. Chin, A secure event update protocol for peer-to-peer massively multiplayer online games against masquerade attacks, *International Journal of Innovative Computing, Information and Control*, Vol.5, No.12 (A) , 2009, pp.4715-4723.

[5] W.-S. Juang, C.-L. Lei, H.-T. Liaw and W.-K. Nien, Robust and efficient three-party user authentication and key agreement using bilinear pairings, *International Journal of Innovative Computing, Information and Control*, Vol.6, No.2, 2010, pp.763-772.

[6] J.-H. Yang and C.-C. Chang, An efficient payment scheme by using electronic bill of lading, *International Journal of Innovative Computing, Information and Control*, Vol.6, No.4, 2010, pp.1773-1780.

[7] J.-Y. Huang, Y.-F. Chung, T.-S. Chen and I-E. Liao, A secure time-bound hierarchical key management scheme based on ECC for mobile agents, *International Journal of Innovative Computing, Information and Control*, Vol.6, No.5, 2010, pp.2159-2170.

[8] C.-T. Li and M.-S. Hwang, An online biometrics-based secret sharing scheme for

multiparty cryptosystem using smart cards, *International Journal of Innovative Computing, Information and Control*, Vol.6, No.5, 2010, pp.2181-2188.

[9] I.-C. Lin, C.-W. Yang and S.-C. Tsaur, Nonidentifiable RFID privacy protection with ownership transfer, *International Journal of Innovative Computing, Information and Control*, Vol.6, No.5, 2010, pp.2341-2352.

[10] H.-C. Hsiang, A novel dynamic ID-based remote mutual authentication scheme, *International Journal of Innovative Computing, Information and Control*, Vol.6, No.6, 2010, pp.2407-2416.

[11] N. W. Lo and K.-H. Yeh, A practical three-party authenticated key exchange protocol, *International Journal of Innovative Computing, Information and Control*, Vol.6, No.6, 2010, pp.2469-2484.

[12] K.-H. Yeh, N. W. Lo and E. Winata, Cryptanalysis of an efficient remote user authentication scheme with smart cards, *International Journal of Innovative Computing, Information and Control*, Vol.6, No.6, 2010, pp.2595-2608.

[13] N. W. Lo and K.-H. Yeh, A novel authentication scheme for mobile commerce transactions, I*nternational Journal of Innovative Computing, Information and Control*, Vol.6, No.7, 2010, pp.3093-3104.

[14] C.-C. Chang and S.-C. Chang, An efficient Internet on-line transaction mechanism, *International Journal of Innovative Computing, Information and Control*, Vol.6, No.7, 2010, pp.3239-3246.

[15] K.-H. Yeh and N. W. Lo, A novel remote user authentication scheme for multi-server environment without using smart cards, *International Journal of Innovative Computing, Information and Control*, Vol.6, No.8, pp.3467-3478, 2010.

[16] J.-L. Tsai, T.-S. Wu, H.-Y. Lin and J.-E. Lee, Efficient convertible multi-authenticated encryption scheme without message redundancy or one-way hash function, *International Journal of Innovative Computing, Information and Control*, Vol.6, No.9, 2010, pp.3843-3852.

[17] H.-L. Wang, T.-H. Chen, L.-S. Li, Y.-T. Wu and J. Chen, An authenticated key exchange protocol for mobile stations from two distinct home networks, *International Journal of Innovative Computing, Information and Control*, Vol.6, No.9, 2010, pp.4125-4132.

[18] J. K. Lee, S. R. Ryu and K. Y. Yoo, Fingerprint-based remote user authentication scheme using smart cards, *IEE Electronics Letters*, Vol.38, No.12, 2002, pp.554-555.

[19] C. H. Lin and Y. Y. Lai, A flexible biometrics remote user authentication scheme, *Computer Standards & Interfaces*, Vol.27, No.1, 2004, pp.19-23.

[20] W. C. Ku, S. T. Chang and M. H. Chiang, Further cryptanalysis of fingerprint based remote user authentication scheme using smartcards, *IEE Electronics Letters*, Vol.41, No.5, 2005, pp.240-241.

[21] E. J. Yoon and K. Y. Yoo, A new efficient fingerprint-based remote user authentication scheme for multimedia systems, *Lecture Notes in Computer Science*, Vol.3684, 2005, pp.332-338.

[22] E. J. Yoon and K. Y. Yoo, Secure fingerprint-based remote user authentication scheme using smartcards, *Lecture Notes in Computer Science*, Vol.3828, 2005, pp.405-413.

[23] 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, 2006, pp.260-268.

[24] M. K. Khan and J. Zhang, Improving the security of 'a flexible biometrics remote user authentication scheme', *Computer standards & Interfaces*, Vol.29, 2007, pp.82-85.

[25] J. Xu, W. T. Zhu and D. G. Feng, Improvement of a fingerprint-based remote user authentication scheme, *International Conference on Information Security and Assurance*, pp.87-92, 2008.

[26] J. Xu, W. T. Zhu and D. G. Feng, Improvement of a fingerprint-based remote user authentication scheme, *scheme*, *International Journal of Security and Its Applications*, Vol.2, 2008, No.3, pp.73-80.

[27] E. J. Yoon, C. J. Yoo. A robust and flexible biometrics remote user authentication scheme. International Journal of Innovative Computing, Information Control Vol. 8, No. 5A, 2012, 3173-3188.