International Journal of Innovative
Computing, Information and Control
Volume **8**, Number **5(A)**, May **2012**

ICIC International ©2012 ISSN 1349-4198
pp. 3173–3188

A ROBUST AND FLEXIBLE BIOMETRICS REMOTE USER AUTHENTICATION SCHEME

Eun-Jun Yoon[1] and Kee-Young Yoo[2,*]

[1]Department of Cyber Security
Kyungil University
33 Buho-Ri, Hayang-Ub, Kyungsan-Si, Kyungsangpuk-Do 712-701, Republic of Korea
ejyoon@kiu.ac.kr

[2]Department of Computer Engineering
Kyungpook National University
1370 Sankyuk-dong, Buk-gu Daegu 702-701, Republic of Korea
*Corresponding author: yook@knu.ac.kr

Received September 2010; revised January 2011

Abstract. *Biometric-based authentication systems are widely deployed for person identification. Recently, an improved scheme for flexible biometrics remote user authentication was proposed by Khan and Zhang. In this paper, we demonstrate that Khan-Zhang's scheme is still vulnerable to the following two attacks: (1) It is insecure to parallel session attack in which an adversary without knowing a legal user's password and biometrics information can masquerade as the legal user by somehow crafting 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 revealed to the insider attacker of the remote system. Moreover, we figure out how to eliminate the security vulnerabilities of Khan-Zhang's scheme. Compared with Khan-Zhang's scheme, the proposed scheme is more efficient and holds stronger security.*
Keywords: Information theory and applications, Cryptography, Biometrics, User authentication, Smart card, Impersonation attack

1. **Introduction.** Remote user authentication scheme is a method to authenticate remote users over insecure communication channel such as Internet [1-7]. Especially, password-based remote user authentication schemes have been widely deployed to authenticate the legitimacy of remote users via the open communication channel [8-22]. However, password-based schemes are vulnerable to the risk of modification and insecurity of password table. Up to now, smart card-based remote user authentication schemes have been proposed to overcome the security problems of the password-based schemes. To provide stronger security, biometric-based remote user authentication schemes with smart cards are also proposed for person identification [23-31].

In 2004, Lin and Lai [24] proposed a flexible biometrics remote user authentication scheme using smart cards. Recently, Khan and Zhang [29], however, pointed out that Lin-Lai's scheme suffers from the server spoofing attack since it does not perform mutual authentication between user and system. In addition, they proposed an improvement of Lin-Lai's scheme that can withstand the attack by adopting mutual authentication technique.

In the security analysis, Khan and Zhang claimed that their improved scheme was secure against various types of attacks. However, we have found that the scheme is still vulnerable to a privileged insider's attack since a legal user's password can be easily revealed to the insider attacker of the remote system [25, 32] and the parallel session attack in which

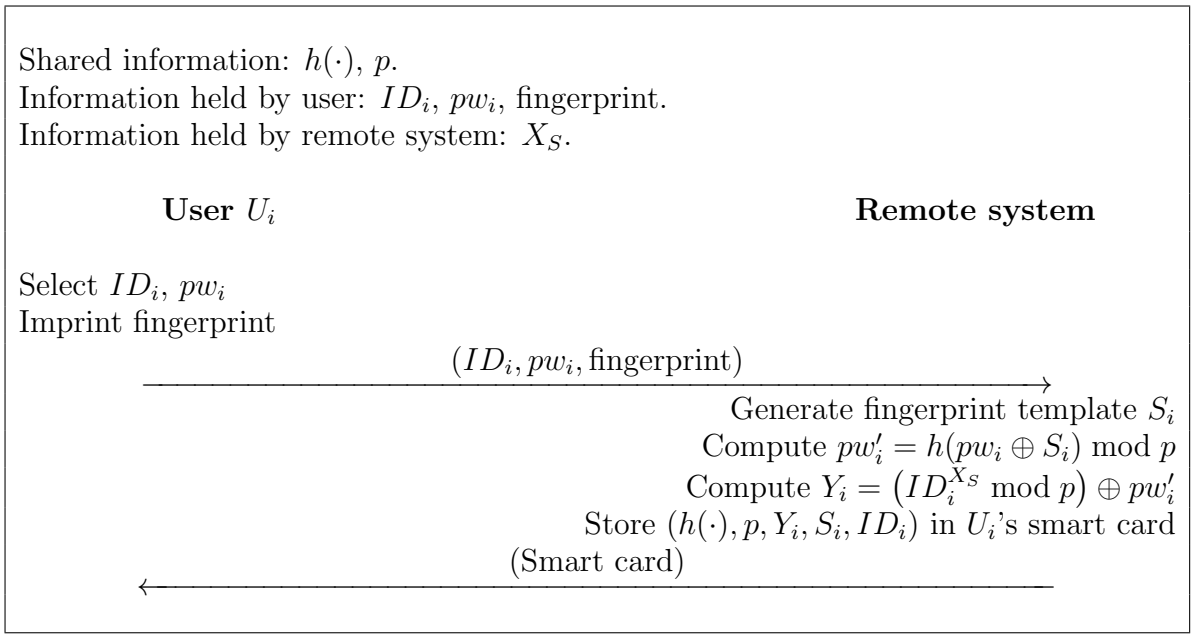

FIGURE 1. Registration phase of Khan-Zhang's scheme

an adversary without knowing a legal user's password and biometrics information can masquerade as the legal user by somehow crafting a valid login message from eavesdropped communications between the user and the remote system [30, 31, 33, 34]. Therefore, this paper demonstrates the vulnerability of the Khan-Zhang's scheme to the privileged insider's attack and the parallel session attack. We also figure out how to eliminate the security vulnerabilities of Khan-Zhang's scheme. As a result, the proposed scheme has better security strength and more efficiency compared with Khan-Zhang's scheme.

The proposed scheme has several important features and advantages as follows. (1) It is designed to optimize the computation cost of each participant by using the small communication round. (2) It achieves cryptographic goals only using bit-wise exclusive-OR (XOR) operation and collision-free one-way hash functions as main cryptographic operations without additional requirements such as using server's public key and digital signatures. (3) It not only is secure against well-known cryptographical attacks such as replay attack, guessing attack, parallel session attack, reflection attack, insider attack and impersonation attack, but also provides mutual authentication and secure password change function without helping of the remote server. Thus, the proposed scheme is very useful in smart card-based Internet and wire/wireless communication environments to access remote information systems since it provides security, reliability and efficiency.

The rest of the paper is organized as follows. Section 2 reviews Khan-Zhang's scheme and then shows the privileged insider's attack and the parallel session attack on the scheme in Section 3. Section 4 presents an improvement of the Khan-Zhang's scheme and discusses the security and efficiency of our improvement in Sections 5 and 6, respectively. Finally, the conclusions come in Section 7.

2. **Review of Khan-Zhang's Authentication Scheme.** This section reviews Khan-Zhang's [29] biometrics remote user authentication scheme. There are four phases in Khan-Zhang's scheme including registration, login, authentication and password change. Figures 1 and 2 show the registration phase and the login and authentication phases of Khan-Zhang's scheme, respectively. Abbreviations used in this paper are as follows:

- U_i: A user.

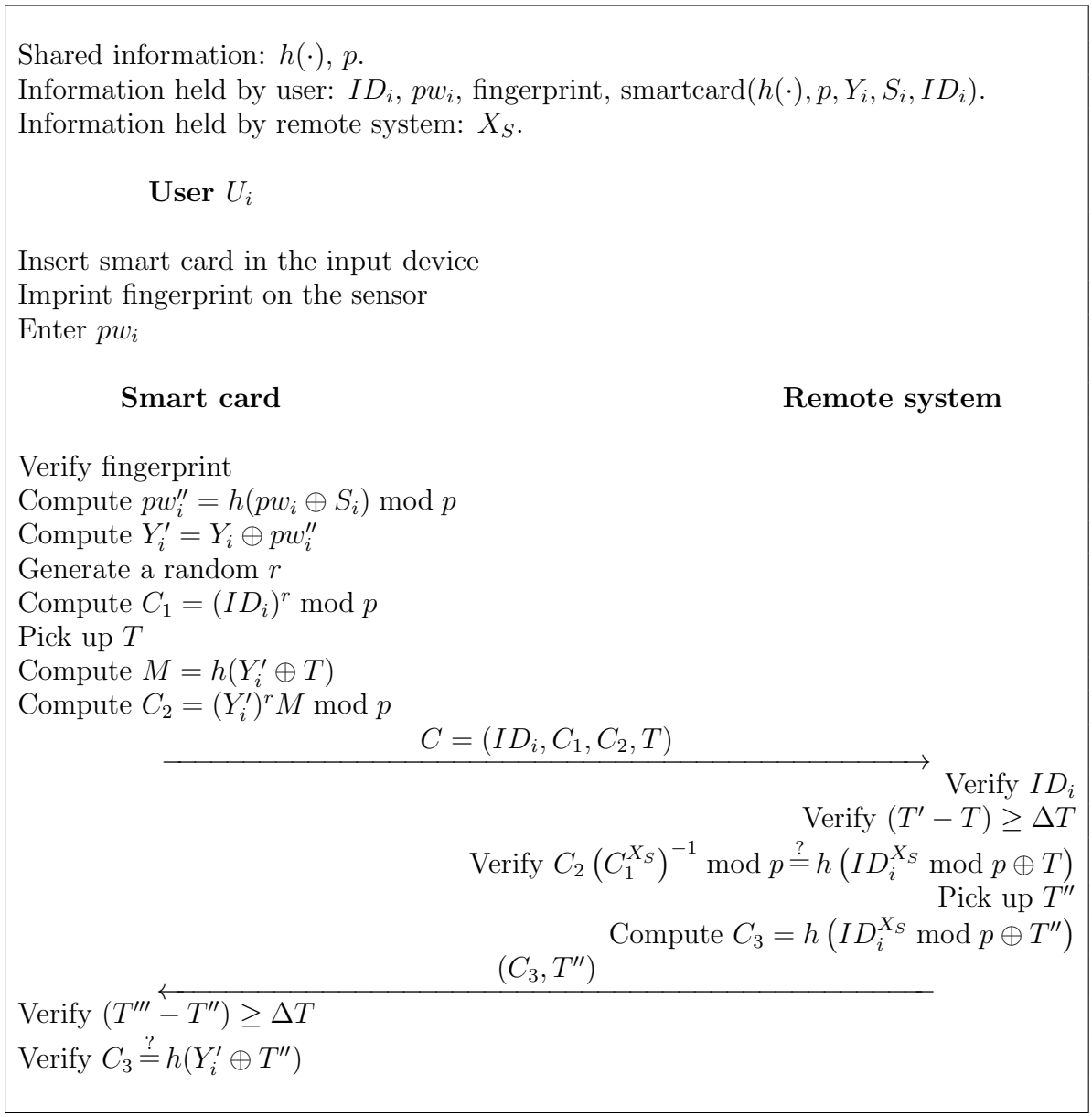

FIGURE 2. Login and authentication phases of Khan-Zhang's scheme

- 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.
- p: Large prime number.
- r: Session-independent random number $\in [1, p-1]$ chosen by U_i.
- 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.** User U_i over a secure channel performs the following operations:

1. Chooses his/her identity ID_i and password pw_i.

2. Personally imprints his/her fingerprint on the sensor.
3. Offers his/her chosen ID_i and pw_i in the registration center.

The remote system of the registration center performs the following operations:

1. Computes
$$pw_i' = h(pw_i \oplus S_i) \bmod p \tag{1}$$
where $h(\cdot)$ denotes collision-free one way hash function, S_i denotes the fingerprint template of U_i, and p is a large prime number.
2. Computes
$$Y_i = \left(ID_i^{X_S} \bmod p\right) \oplus pw_i' \tag{2}$$
where X_S denotes the secret key of the registration server.
3. Issues smart card to the user over a secure channel which contains $h(\cdot)$, p, Y_i, S_i and ID_i.

2.2. **Login phase.** Whenever user U_i wants to login, he/she performs the following operations:

1. Inserts his/her smart card in the input device.
2. Imprints his/her fingerprint on the sensor.
3. Enters his/her password pw_i.

If user U_i passes the fingerprint verification, smart card performs the following operations:

1. Generate a random number r using the minutiae extracted from the imprint fingerprint.
2. Computes $pw_i'' = h(pw_i \oplus S_i) \bmod p$.
3. Computes $Y_i' = Y_i \oplus pw_i''$, where $Y_i' = ID_i^{X_S} \bmod p$.
4. Computes $C_1 = (ID_i)^r \bmod p$.
5. Computes $M = h(Y_i' \oplus T) \bmod p$, where T is the current timestamp of the login device.
6. Computes $C_2 = (Y_i')^r M \bmod p$.
7. Sends login message $C = (ID_i, C_1, C_2, T)$ to the remote system for the authentication process.

2.3. **Authentication phase.** Remote system receives the login message from the user and performs the following operations at time T':

1. Checks whether the format of ID_i is correct or not. If the format is not correct, system rejects the login request.
2. Verifies if $(T' - T) \geq \Delta T$, where ΔT denotes the expected valid time interval for transmission delay, then system rejects the login request.
3. Verifies whether
$$C_2 (C_1^{X_S})^{-1} \stackrel{?}{=} h\left(ID_i^{X_S} \bmod p \oplus\right) \tag{3}$$
or not. If it holds true, system accepts the login request, otherwise login request is rejected.
4. Acquires the current timestamp T''.
5. Computes
$$C_3 = h\left(ID_i^{X_S} \bmod p \oplus T''\right) \tag{4}$$
for mutual authentication.
6. Sends mutual authentication message (C_3, T'') to U_i.

Upon receiving the mutual authentication message (C_3, T''), user U_i performs the following operations at time T''':

1. Verifies if $(T''' - T'') \geq \Delta T$, where T''' is the current timestamp of U_i, then U_i rejects the message.

2. Verifies whether

$$C_3 \stackrel{?}{=} h(Y_i' \oplus T'') \tag{5}$$

or not, where $Y_i' = ID_i^{X_S} \bmod p$ [1)]. If it holds true, U_i believes that the responding party is authentic system and mutual authentication between U_i and remote system is completed, otherwise U_i terminates the connection.

2.4. **Password change phase.** Whenever U_i wants to change the old password pw_i to the new password pw_i^*, he/she has to imprint his/her fingerprint then smart card compares it with the template stored on the smart card. If U_i passes the fingerprint verification, he/she inputs old password pw_i and the new password pw_i^*. The client device performs the following operations:

1. Computes $pw_i'' = h(pw_i \oplus S_i) \bmod p$, where S_i is the fingerprint template stored on the smart card.
2. Computes $Y_i' = Y_i \oplus pw_i'' = ID_i^{X_S} \bmod p$.
3. Computes new $Y_i^* = Y_i' \oplus h(pw_i^* \oplus S_i)$.
4. Replace the old Y_i with the new Y_i^* on the smart card.

3. **Cryptanalysis of Khan-Zhang's Scheme.** This section shows that Khan-Zhang's scheme is vulnerable to parallel session attack [30, 31, 33, 34] and privileged insider attacks [25, 32].

3.1. **Parallel session attack.** This subsection demonstrates that Khan-Zhang's scheme is still vulnerable to the parallel session attack in which an adversary without knowing a legal user's password and biometrics information can masquerade as the legal user by somehow crafting a valid login message from eavesdropped communications between the user and the remote system [30, 31, 33, 34]. A parallel session attack occurs when two or more protocol runs are executed concurrently and messages from one are used to form messages in another session.

A protocol that suffers from a parallel session attack is an example of this: It may be possible to show that the protocol is secure – even when it is under attack – in the case that only a single session of the protocol is deployed on the network. However, when multiple session are present on the network, the parallel session attack can occur because the attacker uses messages from one session to perform the attack on another session [37].

Suppose that an adversary has eavesdropped a valid login request message $C = (ID_i, C_1, C_2, T)$ and mutual authentication message (C_3, T'') from an open network. In the login phase, the adversary can perform the parallel session attack as follows:

1. Puts $C_1^* = 1$.
2. Puts $T^* = T''$, where T'' is the eavesdropped remote system's timestamp and is still "fresh" to the remote system and trickily.
3. Puts $C_2^* = C_3$, where $C_3 = h\left(ID_i^{X_S} \bmod p \oplus T''\right)$.
4. Sends a forged login request message $C^* = (ID_i, C_1^*, C_2^*, T^*)$ to the remote system.

When the remote system receives the message C^*, it will go into the authentication phase and performs the following checks:

[1)] **Comments:** In Steps 3 and 4 of the improved authentication phase, Khan-Zhang [29] described the following arguments: *(Step 3) U_i computes $ID_i^{X_S} \bmod p = Y_i \oplus pw_i'$, where Y_i is stored in the user's smart card and pw_i' is password of the user private to him. (Step 4) U_i computes C_3^* and validates either $C_3^* \stackrel{?}{=} h(ID_i^{X_S} \bmod p \oplus T'')$ or not.* However, Step 3 is unnecessary operation since $ID_i^{X_S} \bmod p (= Y_i')$ is already computed by U_i in Step 3 of the login phase. In addition, the verification equation $C_3^* \stackrel{?}{=} h(ID_i^{X_S} \bmod p \oplus T'')$ of Step 4 is incorrect because U_i received C_3 from the remote system. That is, the verification equation must be changed $C_3^* \stackrel{?}{=} C_3$, where $C_3^* = h(Y_i' \oplus T'') = h(ID_i^{X_S} \bmod p \oplus T'')$.

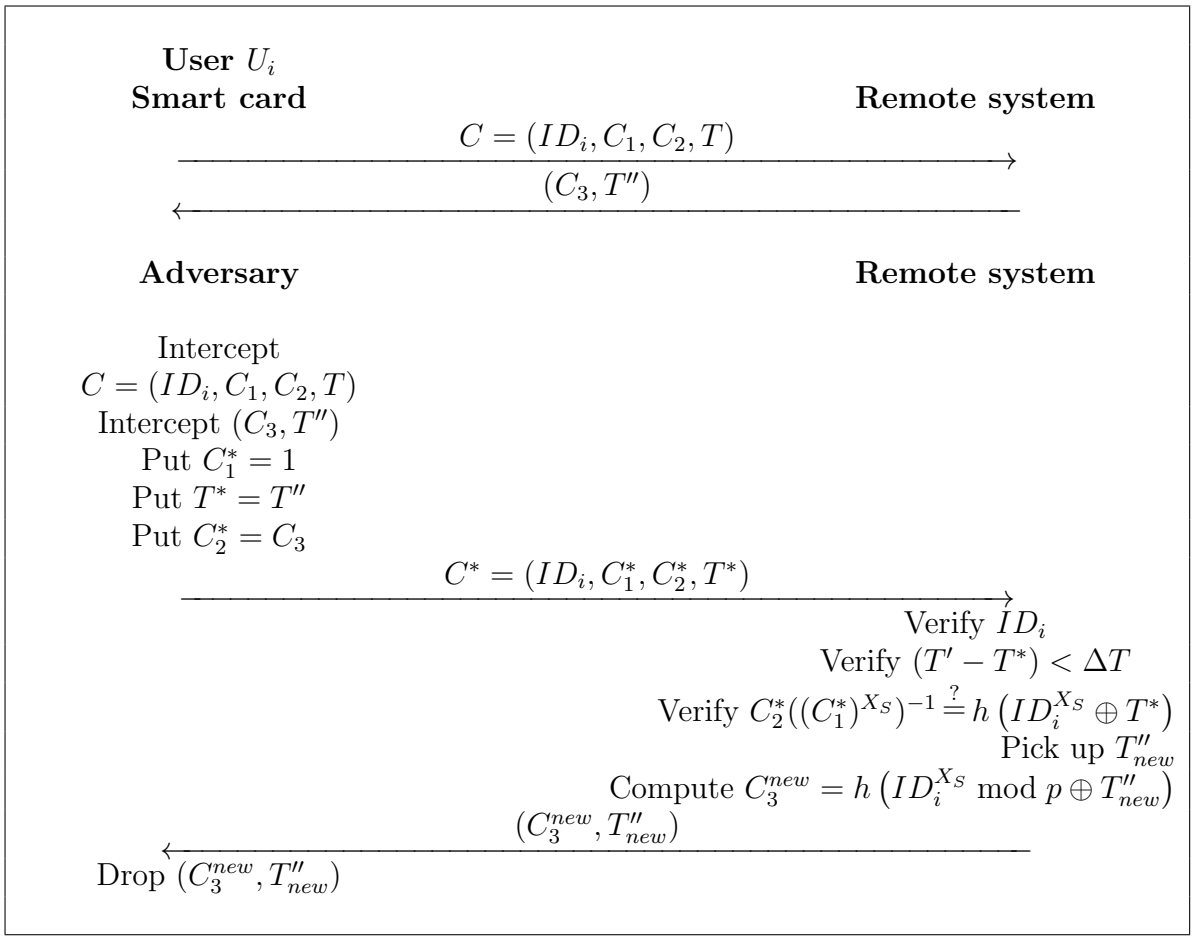

FIGURE 3. Parallel session attack on Khan-Zhang's scheme

1. Checks the format of the ID_i. Of course, it is correct.
2. Checks the time is valid or not. Because $(T' - T^*) < \Delta T$, where T' is the received timestamp of message C^*, the remote system will accept this check.
3. Compares whether

$$C_2^* \left((C_1^*)^{X_S}\right)^{-1} \bmod p \stackrel{?}{=} h\left(ID_i^{X_S} \bmod p \oplus T^*\right). \tag{6}$$

It is easy to see that the adversary can then pass the verification (in parallel with U_i) and thus login the remote system successfully. That is, we can see that the forged login request message C^* will pass the checking of Equation (6) in the authentication phase as follows:

$$\begin{aligned} C_2^* \left((C_1^*)^{X_S}\right)^{-1} \bmod p &= C_2^* \left(1^{X_S}\right)^{-1} \\ &= C_2^*(1)^{-1} \\ &= C_2^* \\ &= C_3 \\ &= h\left(ID_i^{X_S} \bmod p \oplus T^*\right). \end{aligned}$$

For mutual authentication, the remote system will acquire the current timestamp T''_{new} and then compute $C_3^{new} = h\left(ID_i^{X_S} \bmod p \oplus T''_{new}\right)$. Finally, the remote system will send mutual authentication message (C_3^{new}, T''_{new}) to U_i. Then, the adversary intercepts and drops the mutual authentication message (C_3^{new}, T''_{new}) to finish the proposed parallel

session attack. Therefore, the remote system accepts the adversary's forged login request, making Khan-Zhang's scheme insecure.

Figure 3 depicts the messages transmitted in the parallel session attack. We note that such an attack is made possible due to the symmetric nature of the information exchanged between the user and the remote system in the login and authentication phases (i.e., the hash values M and C_3 in Figure 1). For more detail, in the Khan-Zhang's scheme, our parallel session attack could succeed since $M = h(ID_i^{X_S} \bmod p \oplus T')$ of C_1 and $C_3 = h(ID_i^{X_S} \bmod p \oplus T'')$ have the same format. So, if an adversary can get the legal timestamp T^* that can pass the remote system's verification, our attack can easily succeed. Actually, the remote system's timestamp T'' for mutual authentication can easily pass the remote system's verification in the next session. To remedy our parallel session attack, the simple solution is to use M of C_1 and C_3 in different formats.

3.2. **Privileged insider attack.** If a user's password is revealed to a remote server, the insider of the server can impersonate the user to login other remote systems [25, 32]. In practice, users offer the same password to access several servers for their convenience. Thus, the insider of the remote server may try to use the password to impersonate the user to login to other systems that the user has registered with outside this server. If the targeted outside server adopts the normal authentication protocol, it is possible that the insider of the server can successfully impersonate the user to login to it by using a password. Therefore, the password cannot be revealed by the administrator of the server.

However, Khan-Zhang's scheme is vulnerable to privileged insider attacks [25, 32]. In the registration phase of Khan-Zhang's scheme, the user U_i's password pw_i will be revealed to the remote system because it is directly transmitted to the remote system. In practice, users offer the same password pw_i to access several remote servers for their convenience. Thus, a privileged insider of the remote system may try to use U_i's password pw_i to impersonate the legal user U_i to login to the other remote systems that U_i has registered with outside this system.

If the targeted outside remote system adopts the normal password authentication scheme, it is possible that the privileged insider of the remote system could successfully impersonate U_i to login to it by using pw_i. Although it is also possible that all the privileged insiders of the remote system can be trusted and that U_i does not use the same password to access several systems, the implementers and the users of the scheme should be aware of such a potential weakness.

The most familiar example of an insider is a masquerader [38]; an attacker who succeeds in stealing a legitimate user's identity and password and then impersonates another user for malicious purposes. Credit card fraudsters are perhaps the best example of masqueraders. Once a bank customer's commercial identity is stolen (e.g., their credit card or account information), a masquerader presents those credentials for the malicious purpose of using the victim's credit line to steal money.

4. **Proposed Authentication Scheme.** This section presents efficient and secure improvements of Khan-Zhang's scheme to correct the security flaws described in Section 3 and provide more efficiency. To prevent the proposed parallel session attack, the proposed scheme uses the input values of C_1 and C_2 in different formats when performing the login and authentication phases. 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 like Khan-Zhang's scheme. Figures 4 and 5 show

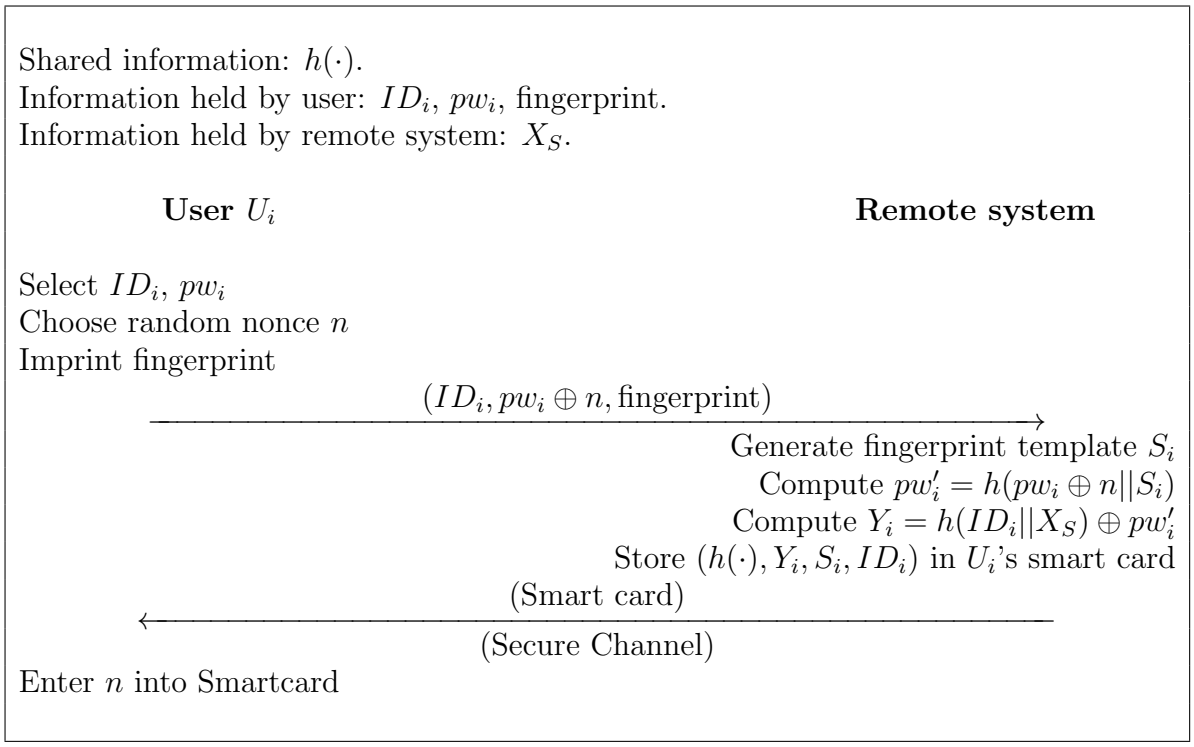

FIGURE 4. Proposed registration phase

the registration phase and the login and authentication phases of the proposed scheme, respectively.

4.1. **Registration phase.** User U_i over a secure channel performs the following operations:

1. Chooses his/her identity ID_i and password pw_i.
2. Generates a random nonce n.
3. Personally imprints his/her fingerprint on the sensor.
4. Offers his/her chosen ID_i and $pw_i \oplus n$ in the registration center.

The remote system of the registration center performs the following operations:

1. Computes
$$pw_i' = h(pw_i \oplus n||S_i) \tag{7}$$
where $h(\cdot)$ denotes collision-free one way hash function and S_i denotes the fingerprint template of U_i.
2. Computes
$$Y_i = h(ID_i||X_S) \oplus pw_i' \tag{8}$$
where X_S denotes the secret key of the registration server.
3. Issues smart card to the user over a secure channel which contains $h(\cdot)$, Y_i, S_i and ID_i.

After receiving the smartcard from remote system, the user U_i enters n into his/her smartcard.

4.2. **Login phase.** Whenever user U_i wants to login, he/she performs the following operations:

1. Inserts his/her smart card in the input device.
2. Imprints his/her fingerprint on the sensor.
3. Enters his/her password pw_i.

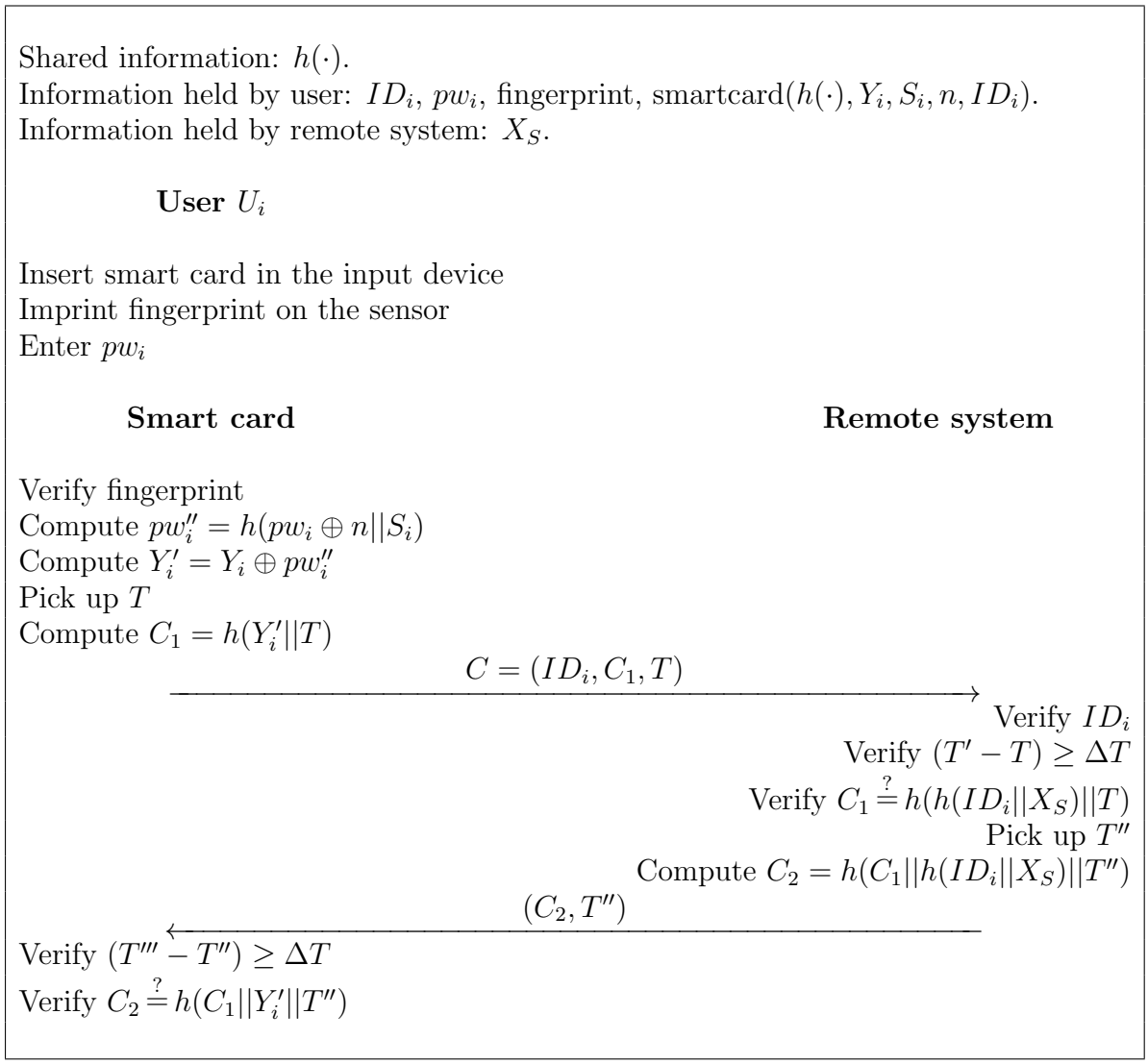

FIGURE 5. Proposed login and authentication phases

If user U_i passes the fingerprint verification, smart card performs the following operations:

1. Computes
$$pw_i'' = h(pw_i \oplus n||S_i) \bmod p \tag{9}$$
and
$$Y_i' = Y_i \oplus pw_i'' \tag{10}$$
where $Y_i' = h(ID_i||X_S)$.
2. Computes
$$C_1 = h(Y_i'||T) \tag{11}$$
where T is the current timestamp of the login device.
3. Sends login message $C = (ID_i, C_1, T)$ to the remote system for the authentication process.

4.3. **Authentication phase.** Remote system receives the login message from the user and performs the following operations at time T':

1. Checks whether the format of ID_i is correct or not. If the format is not correct, system rejects the login request.

2. Verifies if $(T' - T) \geq \Delta T$, where ΔT denotes the expected valid time interval for transmission delay, then system rejects the login request.
3. Verifies whether
$$C_1 \stackrel{?}{=} h(h(ID_i||X_S)||T) \tag{12}$$
or not. If it holds true, system accepts the login request, otherwise login request is rejected.
4. Acquires the current timestamp T''.
5. Computes
$$C_2 = h(C_1||h(ID_i||X_S)||T'') \tag{13}$$
for mutual authentication.
6. Sends mutual authentication message (C_2, T'') to U_i.

Upon receiving the mutual authentication message (C_2, T''), user U_i performs the following operations at time T''':

1. Verifies if $(T''' - T'') \geq \Delta T$, where T''' is the current timestamp of U_i, then U_i rejects the message.
2. Verifies whether
$$C_2 \stackrel{?}{=} h(C_1||Y_i'||T'') \tag{14}$$
or not, where $Y_i' = h(ID_i||X_S)$. If it holds true, U_i believes that the responding party is authentic system and mutual authentication between U_i and remote system is completed, otherwise U_i terminates the connection.

4.4. **Password change phase.** Whenever U_i wants to change the old password pw_i to the new password pw_i^*, he/she has to imprint his/her fingerprint then smart card compares it with the template stored on the smart card. If U_i passes the fingerprint verification, he/she inputs old password pw_i and the new password pw_i^*. The client device performs the following operations:

1. Computes
$$pw_i'' = h(pw_i \oplus n||S_i) \tag{15}$$
where S_i is the fingerprint template stored on the smart card.
2. Extracts a secret value Y_i' as follows:
$$Y_i' = Y_i \oplus pw_i'' = h(ID_i||X_S) \tag{16}$$
3. Computes new secret value Y_i^* as follows:
$$Y_i^* = Y_i' \oplus h(pw_i^* \oplus n||S_i) \tag{17}$$
4. Replace the old Y_i with the new Y_i^* on the smart card.

5. **Security Analysis.** This section discusses the security features of the proposed authentication scheme.

5.1. **Security properties.** The following security properties of the authentication scheme should be considered [25, 32, 34-36].

1. **Replay attack:** A replay attack is an offensive action in which an adversary impersonates or deceives another legitimate participant through the reuse of information obtained in a protocol.

2. **Guessing attack:** A guessing attack involves an adversary (randomly or systematically) trying long-term private keys (e.g., user password or remote system secret key), one at a time, in the hope of finding the correct private key. Ensuring long-term private keys chosen from a sufficiently large space can reduce exhaustive searches. Most users, however, select passwords from a small subset of the full password space. Such weak passwords with low entropy are easily guessed by using the so-called dictionary attack.
3. **Parallel session attack:** The parallel session attack means that an adversary without knowing a user's password can masquerade as the legal user by creating a valid login message from an eavesdropped communication between the authentication server and the user.
4. **Reflection attack:** The reflection attack means that an adversary can masquerade as the legal authentication server by creating a valid response message from an eavesdropped communication between the authentication server and the user.
5. **Privileged insider attack:** When a user's password is revealed to a remote server, the insider of the server can impersonate the user to login other remote systems. In practice, users offer the same password to access several servers for their convenience. Thus, the insider of the remote server may try to use the password to impersonate the user to login to other systems that the user has registered with outside this server. If the targeted outside server adopts the normal authentication protocol, it is possible that the insider of the server can successfully impersonate the user to login to it by using a password. Therefore, the password cannot be revealed by the administrator of the server.
6. **Impersonation attack using lost or stolen smartcards:** An impersonation attack using lost or stolen smartcards means that when legal users lose their smartcards or an adversary steals a smartcard for a short duration and makes a duplicate of it, the attack cannot pass the smartcard verification process. Malicious parties may catch information stored in the smartcard of some user by some ways, such as successfully cracking smartcards that were lost by the user or by obtaining the information in smartcard via illegal card readers or smartcards. With the information stored in smartcards and messages intercepted during previous login transactions between the user and the remote system, the adversarys can pass the authentication process and login to the system successfully.
7. **Mutual authentication:** Mutual authentication means that both the client and server are authenticated to each other within the same protocol.
8. **Secure password change:** Assume a legal user wants to change his/her old password to a new one. If the user's smartcard does not check the validity of the old password, when a smartcard is stolen, unauthorized users can easily change arbitrary new password of the smartcard. And then the legal user's succeeding login requests will be denied unless he/she re-registers with the remote server again. Therefore, the protocol must provide secure password change.

5.2. **Security analysis.** This subsection provides the proof of correctness of the proposed scheme. First, the security terms [35, 36] needed for the analysis of the proposed scheme are defined as follows:

Definition 5.1. *A weak password* (pw_i) *has a value of low entropy, which can be guessed in polynomial time.*

Definition 5.2. *A strong secret key* (X_S) *has a value of high entropy, which cannot be guessed in polynomial time.*

Definition 5.3. *A secure one-way hash function $y = h(x)$ is where a given x to compute y is easy and given y to compute x is hard.*

Under the above three definitions, the following arguments are used to analyze seven security properties [25, 32, 34-36] in the proposed authentication scheme.

Theorem 5.1. *The proposed scheme can resist the replay attack.*

Proof: For replay attacks, the replay of an old login request message $C = \{ID_i, C_1, T\}$ in the authentication phase will not work, as it will fail in step 2 of the remote system's verification process due to the time interval $(T' - T) \geq \Delta T$. In addition, the replay of an old server's response message $(C_2, T''\}$ in the authentication phase will not work, as it will fail in Step 1 of the user's verification process due to the time interval $(T''' - T'') \geq \Delta T$. Therefore, the proposed scheme can resist replay attacks.

Theorem 5.2. *The proposed scheme can resist the guessing attack.*

Proof: Due to the fact that a secure one-way hash function is computationally difficult to invert, it is extremely hard for any adversary to derive X_S from $h(ID_i||X_S)$. Moreover, assume that an adversary intercepts U_i's login request message $C = \{ID_i, C_1, T\}$ and the remote system's response message C_2 over a public network, due to the one-way property of a secure one-way hash function, the adversary cannot derive secret value $Y_i' = h(ID_i||X_S)$ from $C_1 = h(Y_i'||T)$ and $C_2 = h(C_1||h(ID_i||X_S)||T'')$. The password guessing attack will not work against the proposed scheme since the proposed scheme does not use the password for protecting the sending message C_1. Therefore, the proposed scheme can resist guessing attacks.

Theorem 5.3. *The proposed scheme can resist the parallel session attack and the reflection attack.*

Proof: Because of the different message structures between $C_1 = h(Y_i'||T)$ and $C_2 = h(C_1||h(ID_i||X_S)||T'')$, an adversary cannot perform a parallel session attack and reflection attack unlike Khan-Zhang's scheme. Therefore, the proposed scheme can prevent a parallel session attack and reflection attack.

Theorem 5.4. *The proposed scheme can resist the privileged insider attack.*

Proof: Since U_i registers to the remote system by presenting $pw_i \oplus n$ instead of pw_i, an insider of the remote system using an off-line password guessing attack cannot obtain pw_i without knowing the random nonce n. Therefore, without knowing U_i's password pw_i, the adversary cannot succeed the privileged insider attack because he/she need U_i's pw_i to impersonate the legal user and login other remote systems. Therefore, the proposed scheme can resist a privileged insider attack.

Theorem 5.5. *The proposed scheme can resist the impersonation attack using lost or stolen smartcards.*

Proof: Suppose that legal users lose their smartcards or an adversary steals a smartcard for a short duration and makes a duplicate of it. Because the adversary does not know the legal user's password pw_i and the smartcard always verifies the user's fingerprint, the impersonation attack using lost or stolen smartcards cannot pass the smartcard verification process in the login phase. Furthermore, even if an adversary extracts all values $\{h(\cdot), Y_i, S_i, n, ID_i\}$ from the smartcard, the adversary cannot get $h(ID_i||X_S)$ from Y_i without the user's password pw_i. Thus, the proposed scheme prevents an impersonation attack using lost or stolen smartcards.

Theorem 5.6. *The proposed scheme can achieve the mutual authentication.*

Proof: In Step 3 of the proposed authentication phase, the remote system can authenticate U_i. Also, U_i can authenticate the remote system in Step 1 of the authentication phase because only a valid remote system can compute $C_2 = h(C_1||h(ID_i||X_S)||T'')$. Therefore, the proposed scheme can achieve mutual authentication.

Theorem 5.7. *The proposed password change scheme is secure.*

Proof: In the proposed password change phase, the user has to verify himself or herself by a fingerprint biometric, and it is not possible to impersonate a legal user because the biometric is unique. If the input fingerprint is not the same with the stored fingerprint, the user is not allowed to change the password. Moreover, although the smartcard is stolen, unauthorized users cannot change the password. Hence, this scheme is protected from the denial-of-service attack through a stolen device [34]. Therefore, the proposed password change scheme is secure.

The security properties of Khan-Zhang's scheme and of the proposed scheme are summarized in Table 1. Based on the above described cryptanalysis of Khan-Zhang's scheme, Khan-Zhang's scheme is insecure to the parallel session attack and insider attack. Because an adversary can impersonate a legal user by using the proposed parallel session attack, Khan-Zhang's scheme is also insecure to the user impersonation attack. Therefore, we can see that the proposed scheme is more secure in contrast with Khan-Zhang's scheme as shown in Table 1.

Table 1. A comparison of security properties

	Khan-Zhang's Scheme [29]	Proposed Scheme
Replay attack	Secure	Secure
Guessing attack	Secure	Secure
Parallel session attack	Insecure	Secure
Reflection attack	Secure	Secure
Insider attack	Insecure	Secure
Impersonation attack	Insecure	Secure
Mutual authentication	Provide	Provide
Password change	Secure	Secure

6. **Efficiency Analysis.** This section discusses the efficiency features of the proposed scheme. Comparisons between Khan-Zhang's scheme [29] and the proposed scheme are shown in Table 2. To analyze the computational complexity of the proposed scheme, the notation T_{exp} is defined as the time for computing the modular exponentiation, the notation T_{mul} is defined as the time for computing the modular multiplication, the notation T_h is defined as the time for computing the one-way hash function and the notation T_{xor} is defined as the time for computing the bit-wise exclusive-or (XOR) operation.

In the registration phases, Khan-Zhang's scheme requires a total of one exponentiation, one hashing operation and two XOR operations, and the proposed scheme requires a total of two hashing operations and two XOR operations. In the login phase, Khan-Zhang's scheme requires a total of two exponentiations, one multiplication, two hashing operations and three XOR operations, and the proposed scheme requires a total of two hashing operations and two XOR operations. In the authentication phase, Khan-Zhang's scheme requires a total of two exponentiations, two multiplications, three hashing operations

TABLE 2. A comparison of computation costs

	Khan-Zhang's Scheme [29]	Proposed Scheme
Registration phase	$1T_{exp} + 1T_h + 2T_{xor}$	$2T_h + 2T_{xor}$
Login phase	$2T_{exp} + 1T_{mul} + 2T_h + 3T_{xor}$	$2T_h + 2T_{xor}$
Authentication phase	$2T_{exp} + 2T_{mul} + 3T_h + 3T_{xor}$	$4T_h$
Password change phase	$2T_h + 4T_{xor}$	$2T_h + 4T_{xor}$
Communication costs	$\approx$ 2448 bits	$\approx$ 560 bits

and three XOR operations, and the proposed scheme requires a total of four hashing operations. In the password change phase, Khan-Zhang's scheme requires a total of two hashing operations and four XOR operations, and the proposed scheme requires a total of two hashing operations and four XOR operations.

In the login and authentication phases of Khan-Zhang's scheme, among the six transmitted messages $\{ID_i, C_1, C_1, T, C_3, T''\}$, one is the user's identifier (80 bit); two are timestamps (80 bit); two are modular exponentiation bits; and one is hash output bits (160 bit such as a SHA-1 one-way hash function [35, 36]). The total communication costs of Khan-Zhang's scheme is 2448 bits. Unlike Khan-Zhang's scheme, the proposed scheme only uses a minimum communication bandwidth. Among the five transmitted messages $\{ID_i, C_1, T, C_2, T''\}$, one is the user's identifier (80 bit); two are timestamps (80 bit); and two are hash output bits (160 bit). The total communication costs of our scheme is 560 bits. These are very low communication messages. Therefore, the proposed scheme is not only efficient but also enhances security.

7. **Conclusions.** This paper demonstrated that Khan-Zhang's biometric remote user authentication scheme is vulnerable to a privileged insider's attack and Parallel session attack. In order to solve such security problems, this paper also presented an improved scheme to Khan-Zhang's scheme. The proposed scheme has several important features and advantages as follows. (1) It is designed to optimize the computation cost of each participant by using the small communication round. (2) It achieves cryptographic goals only using bit-wise exclusive-OR (XOR) operation and collision-free one-way hash functions as main cryptographic operations without additional requirements such as using server's public key and digital signatures. (3) It not only is secure against well-known cryptographical attacks such as replay attack, guessing attack, parallel session attack, reflection attack, insider attack and impersonation attack, but also provides mutual authentication and secure password change function without helping of the remote server. As a result, the proposed scheme is very useful in smart card-based Internet and wire/wireless communication environments to access remote information systems since it provides security, reliability and efficiency.

Acknowledgements. We would like to thank the anonymous reviewers for their helpful comments. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. 2010-0010106).

REFERENCES

[1] Z. Zhang, B. Fang, M. Hu and H. Zhang, Security analysis of session initiation protocol, *International Journal of Innovative Computing, Information and Control*, vol.3, no.2, pp.457-469, 2007.

[2] Y.-F. Chang, A practical three-party key exchange protocol with round efficiency, *International Journal of Innovative Computing, Information and Control*, vol.4, no.4, pp.953-960, 2008.

[3] C.-Y. Chen, H.-F. Lin and C.-C. Chang, An efficient generalized group-oriented signature scheme, *International Journal of Innovative Computing, Information and Control*, vol.4, no.6, pp.1335-1345, 2008.

[4] J.-S. Lee, Y.-F. Chang and C.-C. Chang, Secure authentication protocols for mobile commerce transactions, *International Journal of Innovative Computing, Information and Control*, vol.4, no.9, pp.2305-2314, 2008.

[5] H.-F. Huang and W.-C. Wei, A new efficient and complete remote user authentication protocol with smart cards, *International Journal of Innovative Computing, Information and Control*, vol.4, no.11, pp.2803-2808, 2008.

[6] C.-L. Chen, Y.-Y. Chen and Y.-H. Chen, Group-based authentication to protect digital content for business applications, *International Journal of Innovative Computing, Information and Control*, vol.5, no.5, pp.1243-1251, 2009.

[7] R.-C. Wang, W.-S. Juang and C.-L. Lei, A robust authentication scheme with user anonymity for wireless environments, *International Journal of Innovative Computing, Information and Control*, vol.5, no.4, pp.1069-1080, 2009.

[8] 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, pp.2657-2664, 2009.

[9] 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), pp.4715-4723, 2009.

[10] 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, pp.763-772, 2010.

[11] 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, pp.1773-1780, 2010.

[12] 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, pp.2159-2170, 2010.

[13] 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, pp.2181-2188, 2010.

[14] 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, pp.2341-2352, 2010.

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

[16] 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, pp.2469-2484, 2010.

[17] 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, pp.2595-2608, 2010.

[18] N. W. Lo and K.-H. Yeh, A novel authentication scheme for mobile commerce transactions, *International Journal of Innovative Computing, Information and Control*, vol.6, no.7, pp.3093-3104, 2010.

[19] 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, pp.3239-3246, 2010.

[20] 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.

[21] 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, pp.3843-3852, 2010.

[22] 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, pp.4125-4132, 2010.

[23] 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, pp.554-555, 2002.
[24] C. H. Lin and Y. Y. Lai, A flexible biometrics remote user authentication scheme, *Computer Standards & Interfaces*, vol.27, no.1, pp.19-23, 2004.
[25] W. C. Ku, S. T. Chang and M. H. Chiang, Further cryptanalysis of fingerprintbased remote user authentication scheme using smartcards, *IEE Electronics Letters*, vol.41, no.5, pp.240-241, 2005.
[26] 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, pp.332-338, 2005.
[27] E. J. Yoon and K. Y. Yoo, Secure fingerprint-based remote user authentication scheme using smartcards, *Lecture Notes in Computer Science*, vol.3828, pp.405-413, 2005.
[28] 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.
[29] M. K. Khan and J. Zhang, Improving the security of 'a flexible biometrics remote user authentication scheme', *Computer standards & Interfaces*, vol.29, pp.82-85, 2007.
[30] 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.
[31] J. Xu, W. T. Zhu and D. G. Feng, Improvement of a fingerprint-based remote user authentication scheme, *International Journal of Security and Its Applications*, vol.2, no.3, pp.73-80, 2008.
[32] W. C. Ku, H. M. Chuang and M. J. Tsaur, Vulnerabilities of Wu-Chieu's improved password authentication scheme using smart cards, *IEICE Trans. Fundamentals*, vol.E88-A, no.11, pp.3241-3243, 2005.
[33] C. L. Hsu, Security of Chien et al.'s remote user authentication scheme using smart cards, *Computer Standards & Interfaces*, vol.26, no.3, pp.167-169, 2004.
[34] E. J. Yoon, E. K. Ryu and K. Y. Yoo, An improvement of Hwang-Lee-Tang's simple remote user authentication scheme, *Computers & Security*, vol.24, pp.50-56, 2005.
[35] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Vanstone, Handbook of Applied Cryptograph*, CRC Press, New York, 1997.
[36] B. Schneier, *Applied Cryptography Protocols, Algorithms and Source Code in C*, 2nd Edition, John Wiley & Sons Inc, 1995.
[37] M. Buchholtz, Automated analysis of infinite scenarios, *International Conference on Trustworthy global Computing*, pp.334-352, 2005.
[38] M. B. Salem, S. Hershkop and S. J. Stolfo, A survey of insider attack detection research, *Insider Attack and Cyber Security: Beyond the Hacker*, pp.69-90, 2008.