ICIC Express Letters
Volume **11**, Number **12**, December **2017**
 ISSN 1881-803X
pp. **1749–1756**

AN IMPROVED USER BIOMETRIC-BASED MULTI-SERVER AUTHENTICATED KEY AGREEMENT SCHEME USING SMART CARDS

Wen-Gong Shieh and Ping Yu*

Department of Information Management
Chinese Culture University
No. 55, Hwa-Kang Rd., Yang-Ming-Shan, Taipei 11114, Taiwan
wgshieh@faculty.pccu.edu.tw; *Corresponding author: yp@faculty.pccu.edu.tw

Received June 2017; accepted September 2017

Abstract. *The use of networks and distributed systems has increased the need for remote user authentication schemes using smart cards. There are many biometric-based multi-server authentication schemes proposed. Among them, Mishra et al. proposed an anonymity-preserving scheme using smart card with the functions of session key agreement, mutual authentication and forward secrecy that is an improvement from Chuang-Chen's scheme. However, we found that Mishra et al.'s scheme is still vulnerable to some attacks. If the attacker is a legal user, even using a not existing user's identity in this system, she/he still can perform the attack. In addition, if the long-term secret of the user is compromised, then all the used session keys will be revealed. Moreover, if the biometric information of a user is compromised, the user's identifier and password will be offline guessed. Based on Mishra et al.'s scheme, we propose an improved scheme to meet the original security and performance requirements. Meanwhile our proposed scheme overcomes the security flaws of Mishra et al.'s scheme.*
Keywords: Authentication, Smart card, Anonymity, Forgery attack, Insider attack, Forward secrecy

1. **Introduction.** In recent years, for the environment of multi-server, remote authentication has been an important issue for network communication. In 2008, Tsai [1] proposed a multi-server authentication scheme using smart cards that does not need to store any verification table in the server and registration center. In 2010, Li and Hwang [2] proposed a biometric-based scheme that was based on the biometrics verification, but Das [3] and Li et al. [4] showed that the Li and Hwang's scheme withstood some design flaws. In 2014, Karuppiah and Saravanan [5] also proposed their remote authentication schemes using smart card, but Shieh and Yu [6] pointed out their scheme is vulnerable to many attacks. In 2014, Mishra et al. [7] showed that Chuang-Chen's [8] multi-server authenticated key agreement scheme based on biometrics does not resist stolen smart card attack which causes the user's impersonation, server spoofing, and denial-of-service attack and proposed a scheme to overcome the weaknesses. However, we found that Mishra et al.'s scheme is still vulnerable to many weaknesses. Firstly, if an attacker registers as a legal user, the attacker can successfully perform user impersonation attack even the user is not registered in the registration center. Secondly, if the user's long-term secret key is compromised, all the session keys of the user can be computed against the property of perfect forward secrecy. Finally, if the biometric information of a user is stolen to fake or reply [9], the attacker can offline guess the correct identity and password. Then, the attacker will successfully perform almost any attacks. Therefore, we propose an enhancement of Mishra et al.'s scheme and provide the criteria of authentication scheme which secures a user against the risk of attack over an insecure Internet environment. Moreover, we

analyze the security of our scheme and prove that ours is suitable for applications with high-security requirements.

The remainder of this paper presents as the following. In the next section, a brief review of Mishra et al.'s scheme is given. After that, we point out the weakness of Mishra et al.'s scheme in Section 3. In Section 4, we propose our improvement scheme and analyze the security in Section 5. Finally, we give our conclusion in the last section.

2. **Review of Mishra et al.'s Scheme.** There are four phases in Mishra et al.'s scheme [7]: the registration, login, authentication, and password change phases as the following. The notations used in this paper are shown in Table 1.

TABLE 1. The notations used in this paper

Notations	Description
RC	Registration center
S_j	Server j
x	A secret value of RC
PSK	A secret key of RC and all S
U_i	User i
U_a	Attacker
SC_i	Smart card of U_i
ID_i	Identity of U_i
SID_i	Identity of S_j
PW_i	Password of U_i
BIO_i	Biometrics of U_i
AID_i	Anonymous identity of U_i
$h(\cdot)$, $H(\cdot)$	One-way hash function
$\oplus$	XOR operator
$\|\|$	Concatenation operator
⟶	a common channel
- - - -▶	a secure channel

2.1. **Registration phase.** The registration of Mishra et al.'s scheme is divided into two sides that servers and users register to the registration center RC. In the server side, RC uses the same PSK to all the authorized servers and facilitates the user's authentication procedure. In the user side, if a user U_i wants to register to an RC, first, U_i chooses the identity ID_i, password PW_i and a random number N_i to compute the value $W_1 = h(PW_i||N_i)$ and $W_2 = h(ID_i||N_i)$. Then, U_i sends ID_i, W_1 and W_2 to RC via a secure channel. If RC accepts the request, RC computes $A_i = h(ID_i||x||T_r)$, $B_i = h(A_i) = h^2(ID_i||x||T_r)$, $X_i = B_i \oplus W_1$, $Y_i = h(PSK) \oplus W_2$ and $Z_i = PSK \oplus A_i$, where T_r is the registration time of U_i, x is the secret key of RC and PSK is the secret key of all servers. Then, RC gives U_i a smart card SC_i containing $\{X_i, Y_i, Z_i, h(.)\}$ via a secure channel. After receiving the SC_i, U_i inserts biometric information BIO_i, computes $N = N_i \oplus H(BIO_i)$ and $V = h(ID_i||N_i||PW_i)$ and inserts N and V in SC_i, $SC_i = \{X_i, Y_i, Z_i, N, V, h(.)\}$, where the one-way hashing function $H(\cdot)$ is designed for user biometric information. The scheme emphasizes that SC_i need not remember the random number N_i. The registration phase is in Figure 1.

2.2. **Login phase.** When U_i wants to log in to the server S_j, U_i inserts SC_i and inputs ID_i, PW_i and BIO_i. The smart card SC_i retrieves $N_i = N \oplus H(BIO_i)$ and computes $V' = h(ID_i||N_i||\ PW_i)$. SC_i checks whether V' is equivalent to the received V. If it fails, SC_i terminates the session. Otherwise, SC_i computes $W_1 = h(PW_i||N_i)$, $W_2 = h(ID_i||N_i)$ and

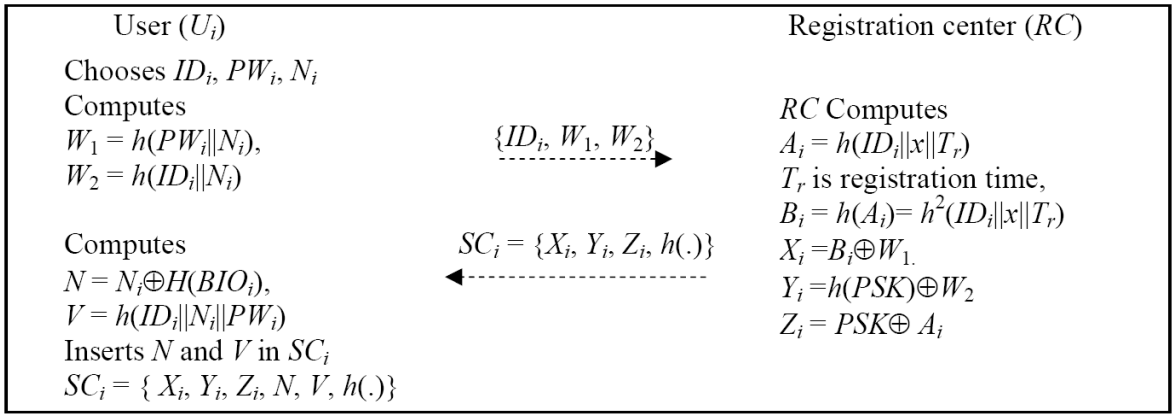

FIGURE 1. The user sider's registration phase of Mishra et al.'s scheme

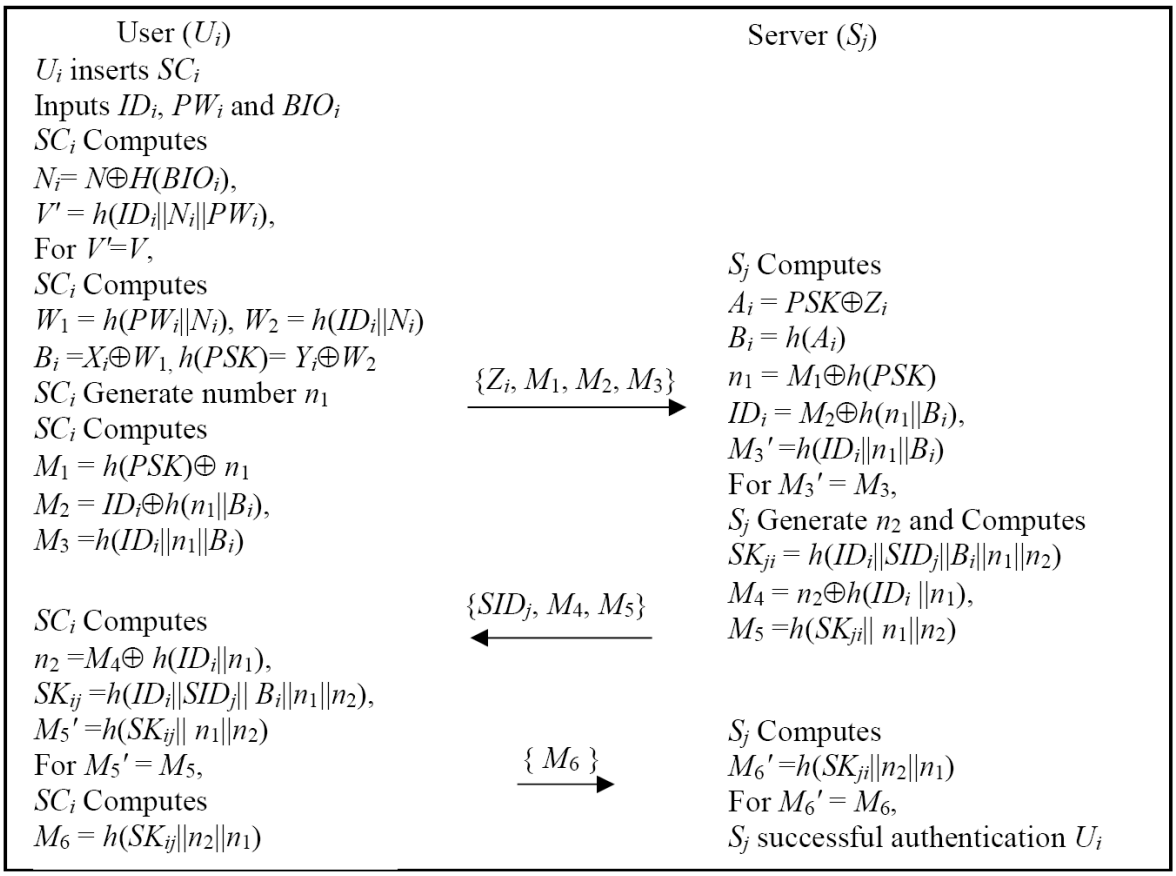

FIGURE 2. Login and authentication phase of Mishra et al.'s scheme

retrieves $B_i = X_i \oplus W_1$, $h(PSK) = Y_i \oplus W_2$. SC_i also generates a random number n_1 and computes $M_1 = h(PSK) \oplus n_1$, $M_2 = ID_i \oplus h(n_1||B_i)$ and $M_3 = h(ID_i||n_1||B_i)$. Then, SC_i sends the message $\{Z_i, M_1, M_2, M_3\}$ to the server S_j. The login phase is shown in Figure 2.

2.3. **Authentication phase.** After receiving the message form U_i, the server S_j retrieves $A_i = PSK \oplus Z_i$, $B_i = h(A_i)$, $n_1 = M_1 \oplus h(PSK)$, $ID_i = M_2 \oplus h(n_1||B_i)$ and checks whether $M_3' = h(ID_i||n_1||B_i)$ is equivalent to the received M_3. If it fails, S_j rejects U_i's login request. Otherwise, it accepts U_i's request. Then, S_j generates a random number n_2 and computes the session key $SK_{ji} = h(ID_i||SID_j||B_i||n_1||n_2)$, $M_4 = n_2 \oplus h(ID_i||n_1)$, $M_5 = h(SK_{ji}||n_1||n_2)$ and sends the message $\{SID_j, M_4, M_5\}$ to U_i. Upon receiving the message from S_j, SC_i retrieves $n_2 = M_4 \oplus h(ID_i||n_1)$, computes $SK_{ij} = h(ID_i||SID_j||B_i||n_1||n_2)$

and checks whether $M_5' = h(SK_{ij}||n_1||n_2)$ is equivalent to the received M_5. If it fails, U_i terminates this session. Otherwise, SC_i computes $M_6 = h(SK_{ij}||n_2||n_1)$ and sends to S_j. After receiving the message, S_j checks whether $M_6' = h(SK_{ji}||n_2||n_1)$ is equivalent to the received M_6. If it fails, S_j rejects U_i's request. Otherwise, S_j successfully authenticates U_i. The authentication phase is shown in Figure 2.

2.4. **Password change phase.** In Mishra et al.'s scheme, the SC_i self can accept the password change request of U_i or not. When U_i wants to change the password, insert SC_i and input ID_i, PW_i and BIO_i. The smart card retrieves $N_i = N \oplus H(BIO_i)$ and checks whether $V' = h(ID_i||N_i||PW_i)$ is equivalent to the stored V. If it fails, SC_i rejects U_i's request. Otherwise, it makes U_i enter PW^{new} and computes $W_1 = h(PW_i||N_i)$, $W_1^{new} = h(PW^{new}||N_i)$, $X_i^{new} = W_1 \oplus W_1^{new}$, $V^{new} = h(ID_i||N_i||PW^{new})$ and replaces X_i, V with X_i^{new} and V^{new}.

3. **Our Attacks of Mishra et al.'s Scheme.** In this section, we demonstrate the weakness of Mishra et al.'s scheme. We follow three assumptions regarding capabilities of an attacker as suggested by Kocher et al. [10], Messerges et al. [11] and Huang et al. [12] respectively. Firstly, an attacker can intercept or modify any message transmitted via a common channel. Secondly, an attacker may steal a user's smart card and retrieve the stored data. Thirdly, the attacker can register as legal users and take legal smart cards. From previous assumptions, we analyze the weakness existing in Mishra et al.'s scheme.

3.1. **The user impersonation attack.** If U_a is a legal user as the third assumption, we can show that an attacker U_a can successfully login to the server S_j using any identity. Because in the Mishra et al.'s scheme, there is a same value $h(PSK)$ in all smart card, using the legal registered smart card $SC_a = \{X_a, Y_a, Z_a, N, V, h(.)\}$ with U_a self-choice identity ID_a, password PW_a and biometric information BIO_a. U_a can compute $N_a = N \oplus H(BIO_a)$, $W_{2a} = h(ID_a||N_a)$ and get the $h(PSK)$ from $h(PSK) = Y_a \oplus W_{2a}$. The U_a also can compute $W_{1a} = h(PW_a||N_a)$ and get B_a from $B_a = X_a \oplus W_{1a}$. Then, U_a generates a random number n_{1b}, using another user's identity ID_b, computes $M_1' = h(PSK) \oplus n_{1b}$, $M_2' = ID_b \oplus h(n_{1b}||B_a)$ and $M_3' = h(ID_b||n_{1b}||B_a)$. Then, the U_a sends the message $\{Z_i, M_1', M_2', M_3'\}$ to the server S_j. After receiving the message from U_a, the server S_j retrieves $A_a = PSK \oplus Z_i$, $n_{1b} = M_1' \oplus h(PSK)$, $ID_b = M_2' \oplus h(n_{1b}||B_a)$, where $B_a = h(A_a)$ and finds $M_3'' = h(ID_b||n_{1b}||B_a)$ equal to the received M_3', because it does not check the ID_a of $A_a = h(ID_a||x||T_r)$ is not equal to the value of ID_b from M_2'. The S_j accepts U_a's request. Then, S_j generates a random number n_2 and computes the session key $SK_{jb} = h(ID_b||SID_j||B_a||n_{1b}||n_2)$, $M_4' = n_2 \oplus h(ID_b||n_{1b})$, $M_5' = h(SK_{jb}||n_{1b}||n_2)$ and sends the message $\{SID_j, M_4', M_5'\}$ to U_a. Upon receiving the message from S_j, U_a retrieves $n_2 = M_4' \oplus h(ID_b||n_1)$, $SK_{bj} = h(ID_b||SID_j||B_a||n_{1b}||n_2)$ and computes $M_6' = h(SK_{bj}||n_2||n_{1b})$ and sends to S_j. After receiving the message, S_j checks if $M_6'' = h(SK_{ja}||n_2||n_{1b})$ is equivalent to the received M_6'. Finally, S_j authenticates U_i. Note that, even if the user uses a not existing user's identity in this system, the attacker still can perform the attack. Hence, Mishra et al.'s scheme cannot provide protection against user impersonation attack.

3.2. **The weakness of biometric information lost.** The biometric information of a user may be compromised from cup or something containing that information by a biometric scanner [9]. In Mishra et al.'s scheme, the user uses the biometric information to protect the identifier and password of a user. Assume that the biometric information BIO_i of U_i is compromised and the attacker gets the value Y_i, N, V of smart card $SC_i = \{X_i, Y_i, Z_i, N, V, h(.)\}$ of U_i. From assumption three as description in Section 3.1, the attacker U_a can register as a legal user. The U_a can offline guess the identifier and password as following steps. Firstly, the U_a retrieves $N_i = N \oplus H(BIO_i)$ and enables to offline guess the identifier ID_i' of U_i, using $W_2' = h(ID_i'||N_i)$. After computing out a value

W_2', U_a can use $Y_i' = h(PSK) \oplus W_2'$ to verify the correctness of identifier. If $Y_i' \neq Y_i$, then U_a repeats with some other guess of ID_i' and so on until he gets success. If $Y_i' = Y_i$, it implies that U_a has successfully guessed U_i's identifier $ID_i' = ID_i$, where Y_i is stored in smart card SC_i. Secondly, after getting the correct ID_i, the U_a enables to offline guess the password PW_i' of U_i. The U_a can use $V' = h(ID_i||N_i||PW_i')$ to verify the correctness of password by comparing the computed V' with the V, where V is known from smart card SC_i. If $V' \neq V$, then U_a repeats with some other guess of PW_i' and so on until he gets success. If $V' = V$, it implies that U_a has successfully guessed U_i's password $PW_i' = PW_i$. Through previous attacks, we find the weaknesses in Mishra et al.'s scheme. If the biometric information is compromised, the user's identifier and password can be offline guessed.

3.3. **Forward secrecy problem.** Mishra et al.'s scheme supposes that attackers cannot compute the established session key $SK_{ji} = h(ID_i||SID_j||B_i||n_1||n_2)$ by using the user U_i's long-term secret key B_i. It supposes that if somehow the secret B_i is compromised, SK_{ji} still remains secure due to the involvement of user's identity ID_i, n_1 and n_2 in its computation because an attacker cannot get those value from either user's smart card or an intercepted login request. However, we find a different conclusion if an attacker U_a is also a legal user of the system and gets the user secret B_i, the successful login message $\{Z_i, M_1, M_2, M_3\}$ of user U_i, and the server S_j's response message $\{SID_j, M_4, M_5\}$. The U_a can compute the session key of this session. From Section 3.1, the U_a is a legal user and can compute the common secret value $h(PSK)$ of all servers in the system. From the value Z_i, M_1 and M_2 in login message, U_a computes $A_i = PSK \oplus Z_i$, $B_i = h(A_i)$, $n_1 = M_1 \oplus h(PSK)$ and $ID_i = M_2 \oplus h(n_1||B_i)$. From the value in the response message of server S_j, U_a can get SID_j, M_4 and compute $n_2 = M_4 \oplus h(ID_i||n_1)$. Therefore, U_a gets all values for session key computation, including ID_i, SID_j, B_i, n_1 and n_2. Hence, Mishra et al.'s scheme cannot provide the forward secrecy for the session key.

3.4. **Mutual authentication problem.** In Mishra et al.'s scheme, the server checks the equivalence of $M_3' = M_3$, but it does not check if the ID_a in $A_a = h(ID_a||x||T_r)$ is equal to the identifier ID_i in M_2'. An attacker can impersonate a user even not existing in the system. Therefore, the Mishra et al.'s scheme does not provide proper mutual authentication.

4. **The Improvement to the Mishra et al.'s Scheme.** In this section, we propose an improvement of the Mishra et al.'s scheme that also provides remote mutual authentication and key agreement scheme using smart card with biometrics. Our scheme also consists of three phases: the registration phase, and the login and verification phase that is described as the following. The symbols in our scheme are defined as the Mishra et al.'s scheme in Table 1.

4.1. **Registration phase.** The registration phase of the improved scheme is similar to Mishra et al.'s scheme which is divided into two sides that servers and users dividedly register to the registration center RC. The server side is the same as Mishra et al.'s scheme, and RC uses the same PSK to all the authorized servers. In the user side, U_i also chooses ID_i, PW_i and a random number N_i to compute the value $W_1 = h(PW_i||N_i)$ and $W_2 = h(ID_i||N_i)$ and sends to RC via a secure channel. If RC accepts the request, RC computes $A_i = h(ID_i||x||T_r)$, $B_i = h(A_i) = h^2(ID_i||x||T_r)$, $X_i = B_i \oplus W_1$, $Y_i = h(PSK||A_i) \oplus W_2$ and $Z_i = PSK \oplus A_i$. Our scheme uses the shared secret value A_i to secret Y_i from the different $h(PSK||A_i)$ between users, even the PSK is the same secret key of all servers. Then, RC gives U_i a smart card SC_i containing $\{X_i, Y_i, Z_i, h(.)\}$ via a secure channel. After receiving the SC_i, U_i inserts biometric information BIO_i, computes $N = N_i \oplus H(BIO_i)$

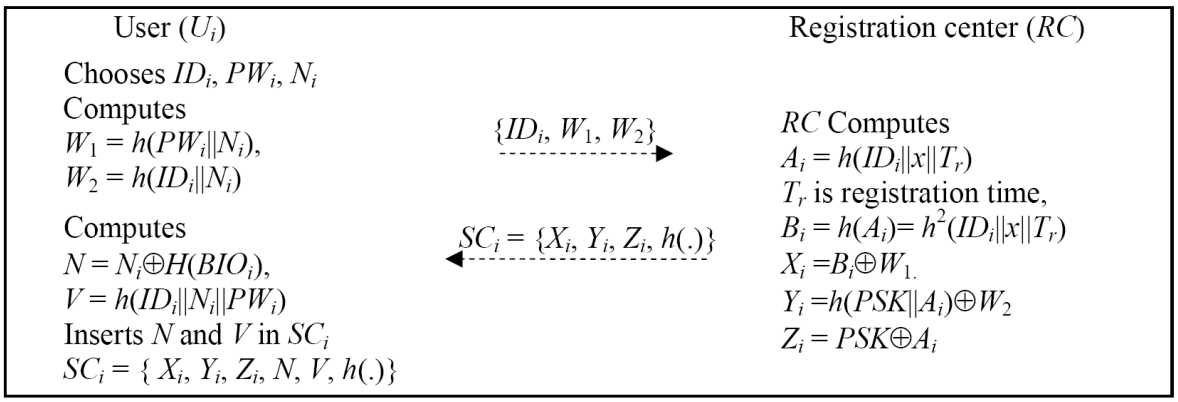

FIGURE 3. The user sider's registration phase of our improved scheme

and $V = h(ID_i||N_i||PW_i)$ and inserts N and V in SC_i, $SC_i = \{X_i, Y_i, Z_i, N, V, h(.)\}$. The registration phase is in Figure 3.

4.2. **Login and authentication phase.** The login phase is similar to Mishra et al.'s scheme. When U_i wants to log in to the server S_j, U_i inserts SC_i and inputs ID_i, PW_i and BIO_i. The smart card SC_i retrieves $N_i = N \oplus H(BIO_i)$ and computes $V' = h(ID_i||N_i||PW_i)$. SC_i checks whether V' is equivalent to the received V. If it fails, SC_i terminates the session. Otherwise, SC_i computes $W_1 = h(PW_i||N_i)$, $W_2 = h(ID_i||N_i)$ and retrieves $B_i = X_i \oplus W_1$, $h(PSK||A_i) = Y_i \oplus W_2$. SC_i also generates a random number n_1 and computes $M_1 = h(PSK||A_i) \oplus n_1$, $M_2 = ID_i \oplus h(n_1||B_i)$ and $M_3 = h(ID_i||n_1||B_i)$. Then, SC_i sends the message $\{Z_i, M_1, M_2, M_3\}$ to the server S_j. After receiving the message from U_i, the server S_j retrieves $A_i = PSK \oplus Z_i$, $B_i = h(A_i)$, $n_1 = M_1 \oplus h(PSK||A_i)$, $ID_i = M_2 \oplus h(n_1||B_i)$ and checks whether $M_3' = h(ID_i||n_1||B_i)$ is equivalent to the received M_3. If it fails, S_j rejects U_i's login request. Otherwise, it accepts U_i's request. Then, S_j generates a random number n_2 and computes the session key $SK_{ji} = h(ID_i||SID_j||B_i||n_1||n_2)$, $M_4 = n_2 \oplus h(ID_i||n_1)$, $M_5 = h(SK_{ji}||n_1||n_2)$ and sends the message $\{SID_j, M_4, M_5\}$ to U_i. Upon receiving the message from S_j, SC_i retrieves $n_2 = M_4 \oplus h(ID_i||n_1)$, computes $SK_{ij} = h(ID_i||SID_j||B_i||n_1||n_2)$ and checks whether $M_5' = h(SK_{ij}||n_1||n_2)$ is equivalent to the received M_5. If it fails, U_i terminates this session. Otherwise, SC_i computes $M_6 = h(SK_{ij}||n_2||n_1)$ and sends to S_j. After receiving the message, S_j checks whether $M_6' = h(SK_{ji}||n_2||n_1)$ is equivalent to the received M_6. If it fails, S_j rejects U_i's request. Otherwise, S_j successfully authenticates U_i. Our improved scheme of login and authentication phase shows in Figure 4. The password change phase is similar to Mishra et al.'s scheme, so we do not repeat here.

5. **Security and Efficiency Analysis.** In this section, we analyze the security and performance of our improved scheme. Our scheme is similar to the Mishra et al.'s scheme, but does not inherit their weaknesses. Therefore, the user impersonation attack, biometric information lost to guess identifier and password and forward secrecy problem can be avoided. In our improved scheme, each user is with different $h(PSK||A_i)$ from $A_i = h(ID_i||x||T_r)$ that confirm the different users have different shared secret key to the server. Because in the Mishra et al.'s scheme, there is the same value $h(PSK)$ in all smart cards that the attack can register as legal users and take many attacks, the same, without the $h(PSK||A_i)$, the attacker cannot verify the correctness of identifier and is not able to offline guess the password. Additionally, without knowing the identifier of a user, the attacker is impossible to create session key. Hence, our scheme can provide the perfect forward secrecy.

The computation costs of our proposed scheme and Mishra et al.'s scheme are almost the same except that our scheme adds two concatenation operations in the registration

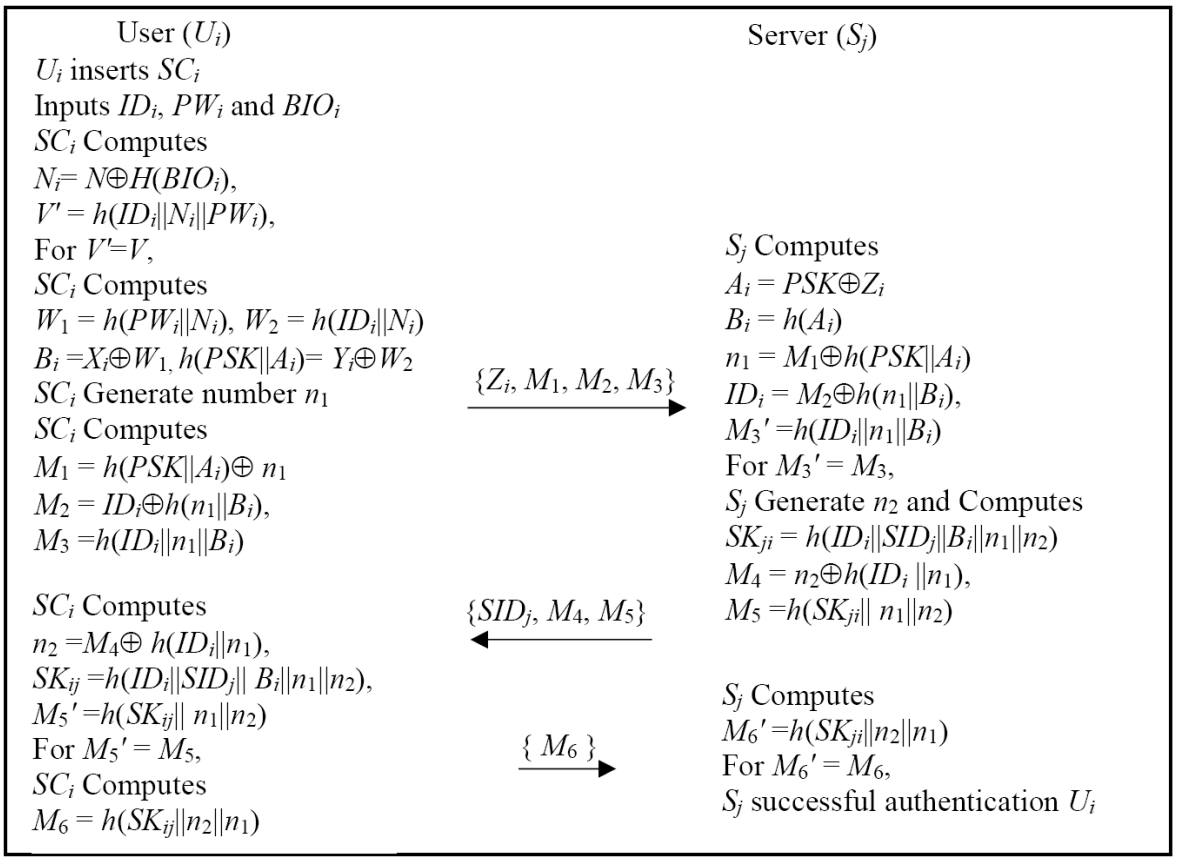

FIGURE 4. Login and authentication phase of our improved scheme

and authentication phases. That is, our scheme has similar performance as Mishra et al.'s scheme but without their weaknesses.

6. **Conclusion.** We analyze the weaknesses of the remote user authentication scheme proposed by Mishra et al. Through entire analysis, we find that Mishra et al.'s scheme may be not suitable for applications in the network that require user privacy and security. Therefore, we propose an improvement of Mishra et al.'s scheme, an attacker cannot obtain any sensitive information, even if she/he is a malicious legal user. The enhancement scheme is still based on one-way hash functions and not only inherits the merits of their scheme but also enhances the security of their scheme. Thus, the user impersonation attack, biometric information lost to offline-guessing identifier and password and forward secrecy problem are completely solved. Therefore, our scheme holds substantial value in the context of numerous applications in various network environments. For future research directions it is based on different aspects like password table, biometric and smart card for authenticating the remote user. To make the most reliable scheme, it is important to calculate computational and communication cost. Also, it requires resistance against many other threats. For the mutual authentication and communication privacy it is the most essential requirements for remote user authentication scheme.

REFERENCES

[1] J.-L. Tsai, Efficient multi-server authentication scheme based on one-way hash function without verification table, *Computers & Security*, vol.27, pp.115-121, 2008.

[2] 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.

[3] A. K. Das, Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards, *Information Security IET*, vol.5, pp.145-151, 2011.

[4] X. Li, J.-W. Niu, J. Ma, W.-D. Wang and C.-L. Liu, Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards, *Journal of Network and Computer Applications*, vol.34, pp.73-79, 2011.
[5] M. Karuppiah and R. Saravanan, A secure remote user mutual authentication scheme using smart cards, *Journal of Information Security and Applications*, vol.19, pp.282-294, 2014.
[6] W.-G. Shieh and P. Yu, The weaknesses of Karuppiah et al.'s remote user mutual authentication scheme using smart card, *ICIC Express Letters*, vol.10, no.12, pp.2817-2822, 2016.
[7] D. Mishra, A. K. Das and S. Mukhopadhyay, A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards, *Expert Systems with Applications*, vol.41, pp.8129-8143, 2014.
[8] M.-C. Chuang and M. C. Chen, An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics, *Expert Systems with Applications*, vol.41, pp.1411-1418, 2014.
[9] A. K. Jain, A. Ross and S. Pankanti, Biometrics: A tool for information security, *IEEE Trans. Information Forensics and Security*, vol.1, pp.125-143, 2006.
[10] P. Kocher, J. Jaffe and B. Jun, Differential power analysis, *Proc. of Advances in Cryptology*, 1999.
[11] T. S. Messerges, E. A. Dabbish and R. H. Sloan, Examining smart-card security under the threat of power analysis attacks, *IEEE Trans. Computers*, vol.51, pp.541-552, 2002.
[12] X. Huang, X. Chen, J. Li, Y. Xiang and L. Xu, Further observations on smart-card-based password-authenticated key agreement in distributed systems, *IEEE Trans. Parallel and Distributed Systems*, vol.25, pp.1767-1775, 2014.