A Lightweight Authentication and Key Agreement Scheme for Telecare Medicine Information System

Jung-Wen Lo, Chun-Yueh Wu, Shu-Fen Chiou

Department of Information Management, National Taichung University of Science and Technology, Taiwan
asalo@nutc.edu.tw, ted811004@gmail.com, sfchiou@nutc.edu.tw

Abstract

With the advancement of Internet of Thing, the telecare medicine information system provides efficient and convenient healthcare services for patients. However, it has also spawned many privacy and security issues. Recently, Amin and Biswas pointed out that the scheme proposed by Giri et al. is vulnerable to offline password-guessing attacks and insider attacks and fails to protect user anonymity, and they proposed an improved scheme. Arshad and Rasoolzadegan pointed out that the scheme proposed by Amin and Biswas cannot withstand offline password-guessing attacks and replay attacks and cannot provide perfect forward secrecy. This article shows that the scheme proposed by Arshad and Rasoolzadegan does not allow changing one's own password offline. Therefore, we propose a new scheme to solve this problem and improve efficiency and security.

Keywords: IoT, TMIS, Elliptic curve cryptography, Authentication

1 Introduction

Due to the popularity of the Internet of Things, it has improved the convenience of life, especially for health care. Many instant physiological information is available through a variety of sensing devices. In addition, the pattern of the world's medical industry has undergone many changes from the original clinical medical services to home and preventive care. Medical services can now be provided remotely by measuring patients' physiological information at any place and time and transmitting it back to the hospital via devices to allow doctors to determine the disease conditions. Therefore, measurement of physiological information by patients at home is gradually becoming a trend. The Telecare Medicine Information System (TMIS) can also allow patients with chronic illness to prevent disease symptoms more effectively.

However, while these advancements have brought about convenient applications, they have also led to security problems, especially in the TMIS system, where the patients' right to privacy requires more attention. Generally, the public channel through which users access medical services is considered insecure. Therefore, remote users and servers must use an account and password to authenticate each other, an encryption/decryption mechanism must be used to ensure transmission security of the public channel, and a key exchange mechanism must be applied for obtaining the session key. From 2010 to 2012, many proposed improved schemes with dual-factor authentication via an account and password plus a smartcard [6, 14, 17-18, 20]. However, most of these schemes did not achieve user anonymity, and user identity may be known through eavesdropping or attacks. Therefore, from 2012 to 2018, many proposed improved schemes for identity authentication with enhanced anonymity [1-5, 7, 9-13, 15, 18-19].

To reduce the threat from attackers and improve the effectiveness of the scheme, in 2015, Mishra et al. developed a good authentication mechanism to satisfy the following requirements: (1) Quick detection of errors at the login phase, (2) Enabling change of one's password offline, (3) Improved user anonymity, (4) Providing a session key agreement and mutual authentication function, (5) Lower communication costs and computing costs, and (6) Meeting all security requirements [16].

We found that the scheme proposed by Arshad and Rasoolzadegan for TMIS only allows changing one's own password online [2]. Therefore, to achieve the above mentioned requirements of a good authentication mechanism, we proposed an improved authentication scheme.

The remaining sections of this article are organized as follows. Section 2 mainly reviews literature related to TMIS encryption and authentication technology. Section 3 briefly reviews the scheme proposed by Arshad and Rasoolzadegan. We propose our authentication scheme in Section 4 and discuss its security in Section 5. In Section 6, we discuss the costs of our scheme and other related schemes. Section 7 is the conclusion.

*Corresponding Author: Jung-Wen Lo; E-mail: asalo@nutc.edu.tw
DOI: 10.3966/160792642020012101022

2 Literature Review

In recent years, the encryption and authentication technology for TMIS has become increasingly sophisticated. Wu et al. proposed an authentication scheme in 2010, adding a pre-computing step and noted that the computing cost of his own design scheme was lower than previous proposals [19]. However, He et al. found that Wu et al.'s scheme was prone to insider and impersonation attacks, so they proposed a more secure authentication scheme to overcome these shortcomings [6]. Nevertheless, in 2012, Wei et al. noted deficiencies in the schemes proposed by Wu et al. and He et al., because these two password-based authentication schemes did not perform well and did not satisfy the two-factor authentication. Therefore, Wei et al. proposed a more efficient two-factor authentication scheme [17]. Later, Zhu noted that Wei et al.'s scheme could not resist offline password-guessing attacks. They proposed an improved scheme to overcome these shortcomings [21].

The above works proposed authentication schemes for TMIS to solve the problem of dual-factor authentication, but none of them achieved protection of user anonymity. User anonymity means that users' data cannot be known to people on the network. If an attacker retrieves a message from the message channel, the user's data will not be disclosed through decryption. An authentication scheme must ensure user anonymity and prevent misuse by attackers. To achieve user anonymity in identity authentication, Chen et al. proposed a TMIS scheme based on identity authentication in 2012, which can protect users' sensitive information and requires less computing cost [5]. However, Zhai and Cao showed that Chen et al.'s scheme is vulnerable to online and offline password-guessing attacks. Therefore, they proposed an improved authentication scheme to resist guessing attacks [3]. Xie et al. also showed that Chen et al.'s scheme is vulnerable to impersonation attacks and offline password-guessing attacks, so they proposed a new TMIS scheme to address these weaknesses [20]. Lin also demonstrated that, if Chen et al.'s scheme encounters dictionary attacks, the passwords can be cracked, and proposed a new password-based anonymous authentication scheme [13]. However, Mishra noted that, although these schemes are effective in protecting user anonymity and resisting password-guessing attacks, they do not provide a highly efficient login phase and a friendly password-changing phase. The above schemes cannot judge the correctness of input during the registration and login verification phases, which may lead to denial-of-service attacks [15].

Giri et al. proposed an improved authentication scheme in 2015 to resist various attacks [7]. However, Amin and Biswas noted that Giri et al.'s scheme is vulnerable to offline password guessing and insider attacks and fails to protect user anonymity, so they proposed an improved scheme [1]. However, Arshad and Rasoolzadegan noted that Amin and Biswas's scheme is vulnerable to offline password-guessing and replay attacks and cannot provide perfect forward secrecy. They also noted that Giri et al.'s scheme not only has the weaknesses noted by Arshad and Rasoolzadegan but also is vulnerable to replay attacks and does not provide perfect forward secrecy [2].

3 Scheme Proposed by Arshad and Rasoolzadegan

Generally, among all the TMIS schemes we searched, we found that the scheme proposed by Arshad and Rasoolzadegan to be superior. In this Section, we elaborate on their scheme.

3.1 Definitions of Symbols

The notations of the symbols used in this article are summarized in Table 1. U_i is a user or patient, and S is a server or hospital. At the beginning, we selected an elliptic curve $E_p(a,b)$, a point on the elliptic curve P, and two collision-free one-way hash functions $h_1(\cdot)$ and $h_2(\cdot)$ and the Bio-hash function $\mathrm{H}(\cdot)$.

Table 1. Notations of symbols

Symbol	Description
ID_i	Identity of User i
CID_i	Dynamic identity of User i
PW_i	Password of User i
b_i	Random number generation by User i
$h(\cdot)$	Collision-free one-way hash function
$\|\|$	Concatenation operator
$\oplus$	XOR operator
P	A point on elliptic curve $E_p(a,b)$
T	Timestamp
s	Private key of Server
$E_s(\ )/D_s(\ )$	Symmetric encryption/decryption
SK	Shared session key between user and server

3.2 Registration Phase

This phase is mainly to provide the detailed steps for registering and obtaining a smartcard (see Figure 1):

(1) The user enters his/her identity ID_i and password PW_i and generates a random number b_i. Then, $PWb_i = h(PW_i \| b_i)$ is calculated, and $[ID_i, PWb_i]$ is sent to the server through the secure channel.

(2) The server receives the message $[ID_i, PWb_i]$ and checks whether the database ID_i exists. If it exists, the user will be requested to select another ID_i; if not, the

server generates a random number r; calculates $R_i = h(ID_i \| s)$, $A_i = R_i \oplus h(ID_i \| PWb_i)$, and $CID_i = E_s(ID_i \| r)$, respectively; saves ID_i in the database; saves $\{A_i, CID_i, E, P, h(\ )\}$ in the memory of the smartcard; and gives the smartcard to the user through the secure channel.

(3) When the user receives the smartcard, he/she stores the random number b_i in the smartcard memory.

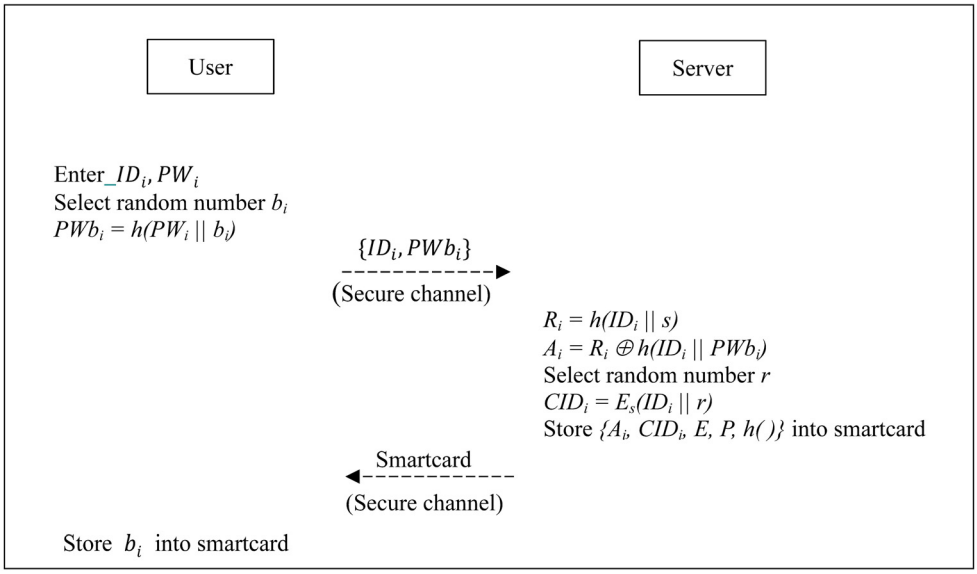

Figure 1. Registration phase of the scheme proposed by Arshad and Rasoolzadegan

3.3 Login and Verification Phase

This phase mainly involves steps for user login and verification (see Figure 2).

(1) The user inserts his/her smartcard into the card reader and enters his/her ID_i and PW_i. Then, a random number k_1 is selected, and $K_1 = k_1 P$, $R_i = A_i \oplus h(ID_i \| h(PW_i \| b_i))$ and $V_1 = h(ID_i \| K_1 \| R_i \| T_1)$ are calculated. Then, the login message $\{CID_i, K_1, V_i, T_1\}$ is transmitted to the server through the public channel, where T_1 is the current timestamp.

2) When the server receives the message $\{CID_i, K_1, R_i, T_1\}$, it will first check the validity of the timestamp T_1. If it is within the validity, it will calculate D_s (CID_i) to obtain $(ID_i \| r)$ and verify whether $h(ID_i \| K_i \| h(ID_i \| s) \| T_1)$ equals V_i; if not, the session will be terminated; if so, it will obtain the random numbers k_2, and r^{new} and calculate $CID_i^{new} = E_s(ID_i \| r^{new})$, $K_2 = k_2 P$, $K = k_2 K_1$, $ECID_i = h(K) \oplus CID_i^{new}$, and $V_2 = h(K_1 \| h(ID_i \| s) \| K_2 \| CID_i^{new} \| K)$. After the calculation, the message $\{K_2, ECID_i, V_2\}$ is sent to the user through the public channel.

(3) When the user receives the message $\{K_2, ECID_i, V_2\}$, K = $k_1 K_2$ and $CID_i^{new} = h(K) \oplus ECID_i$ are calculated, and whether $h(K_1 \| R_i \| K_2 \| CID_i^{new} \| K)$ equals V_2 is checked; if not, the session will be terminated; if so, $V_3 = h(R_i \| V_2 \| K)$ is calculated, and CID_i in the smartcard is replaced with CID_i^{new}. Then, $\{V_3\}$ is transmitted to the server through the public channel, and the session key is finally calculated as $h(ID_i \| K \| K_1 \| K_2)$.

(4) When the server receives the message $\{K_2, ECID_i, V_2\}$, it checks whether $h(h(ID_i \| s) \| V_2 \| K)$ equals V_3; if not, the server rejects this message; if so, the server approves the user's login authentication and calculates the session key $h(ID_i \| K \| K_1 \| K_2)$.

3.4 Password Changing Phase

If the user wants to change the password, he/she should input his/her account ID_i, the old password PW_i, and the new password PW_i^{new} to the system. The detailed steps are as follows.

(1) The same as in the step 1 of login and verification phase

(2) The same as in the step 2 of login and verification phase

(3) When the user receives the message $\{K_2, ECID_i, V_2\}$, K = $k_1 K_2$ and $CID_i^{new} = h(K) \oplus ECID_i$ are calculated, and whether $h(K_1 \| R_i \| K_2 \| CID_i^{new} \| K)$ equals V_2 is checked; if not, the attempt is rejected; if so, $A_i^{new} = A_i \oplus h(ID_i \| h(PW_i \| b_i)) \oplus h(ID_i \| h(PW_i^{new} \| b_i))$ is calculated, and CID_i and A_i in the smartcard are replaced with CID_i^{new} and A_i^{new}.

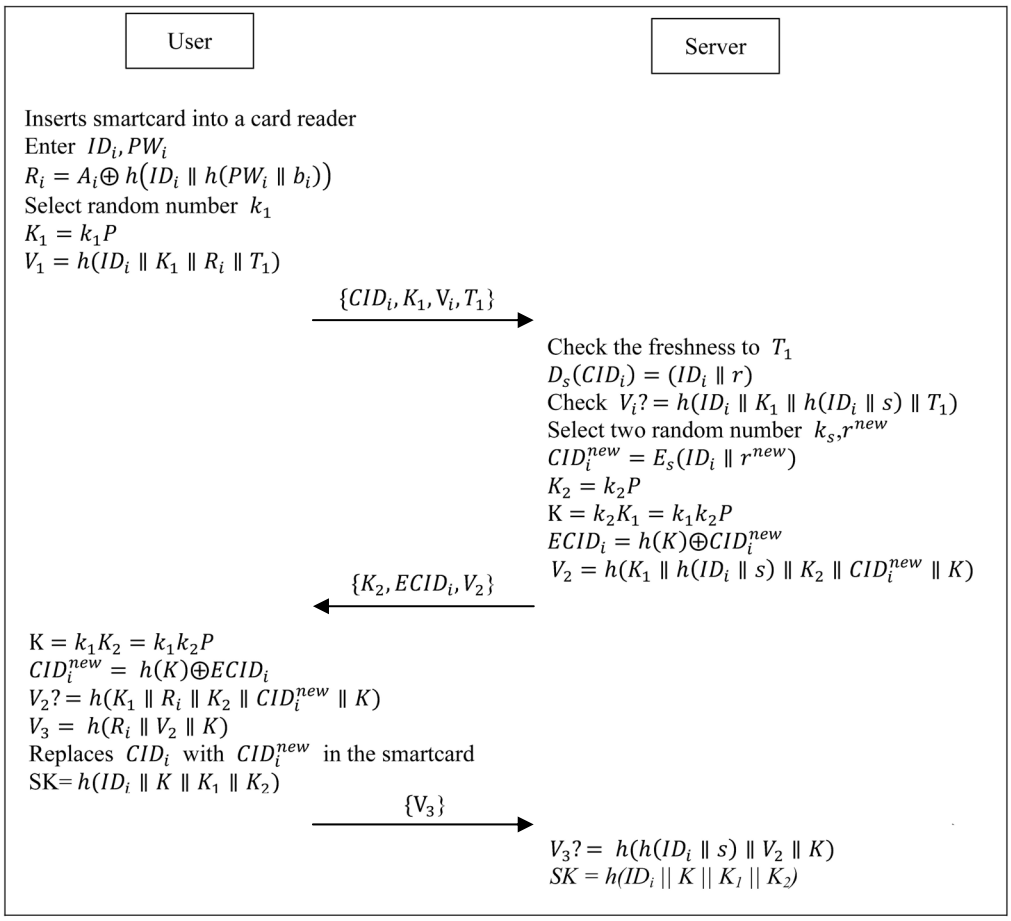

Figure 2. Login and verification phase of the scheme proposed by Arshad and Rasoolzadegan

4 Proposed Scheme

We found that the Arshad-Rasoolzadegan scheme does not allow changing one's own password offline so their scheme will increase the cost of communication. Therefore, we proposed an improved scheme. The scheme is still divided into three phases: registration, login and verification, and password change. At the registration phase, the user registers with the server. At the login and verification phase, the user transmits a login request to the server, and the identity is verified. The password-changing phase is used when the user requirements to change the password.

4.1 Registration Phase

In the proposed scheme, this phase mainly involves providing detailed steps for registration and obtaining a smartcard (see Figure 3).

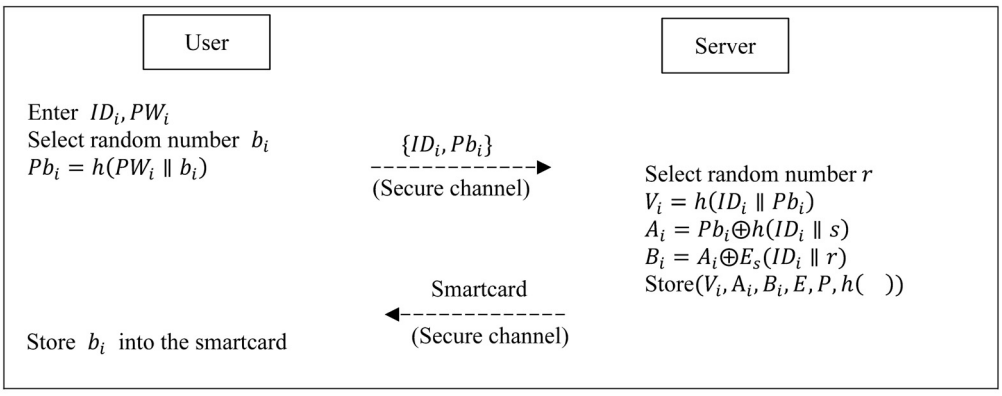

Figure 3. Registration phase of the proposed scheme

(1) The user enters his/her identity ID_i and password PW_i and generates a random number b_i Then, $pb_i = h(PW_i \| b_i)$ is calculated, and $\{ID_i, Pb_i\}$ is sent to the server through the secure channel.

(2) The server receives the message $\{ID_i, Pb_i\}$. The server checks whether the database ID_i exists. If it

exists, the user will be asked to select another ID_i. If it does not, the server will generate a random number r and calculate $V_i = h(ID_i \| Pb_i)$, $A_i = Pb_i \oplus h(ID_i \| s)$ and $B_i = A_i \oplus E_2(ID_i \| r)$, save ID_i in the database, save $\{V_i, A_i, B_i, E, P, h(\ )\}$ in the memory of the smartcard, and give the smartcard to the user through the secure channel, such as face to face delivery.

(3) When the user receives the smartcard, the random number b_i is stored in its memory.

4.2 Login and Verification Phase

In the proposed scheme, this phase mainly involves user login and verification steps (see Figure 4).

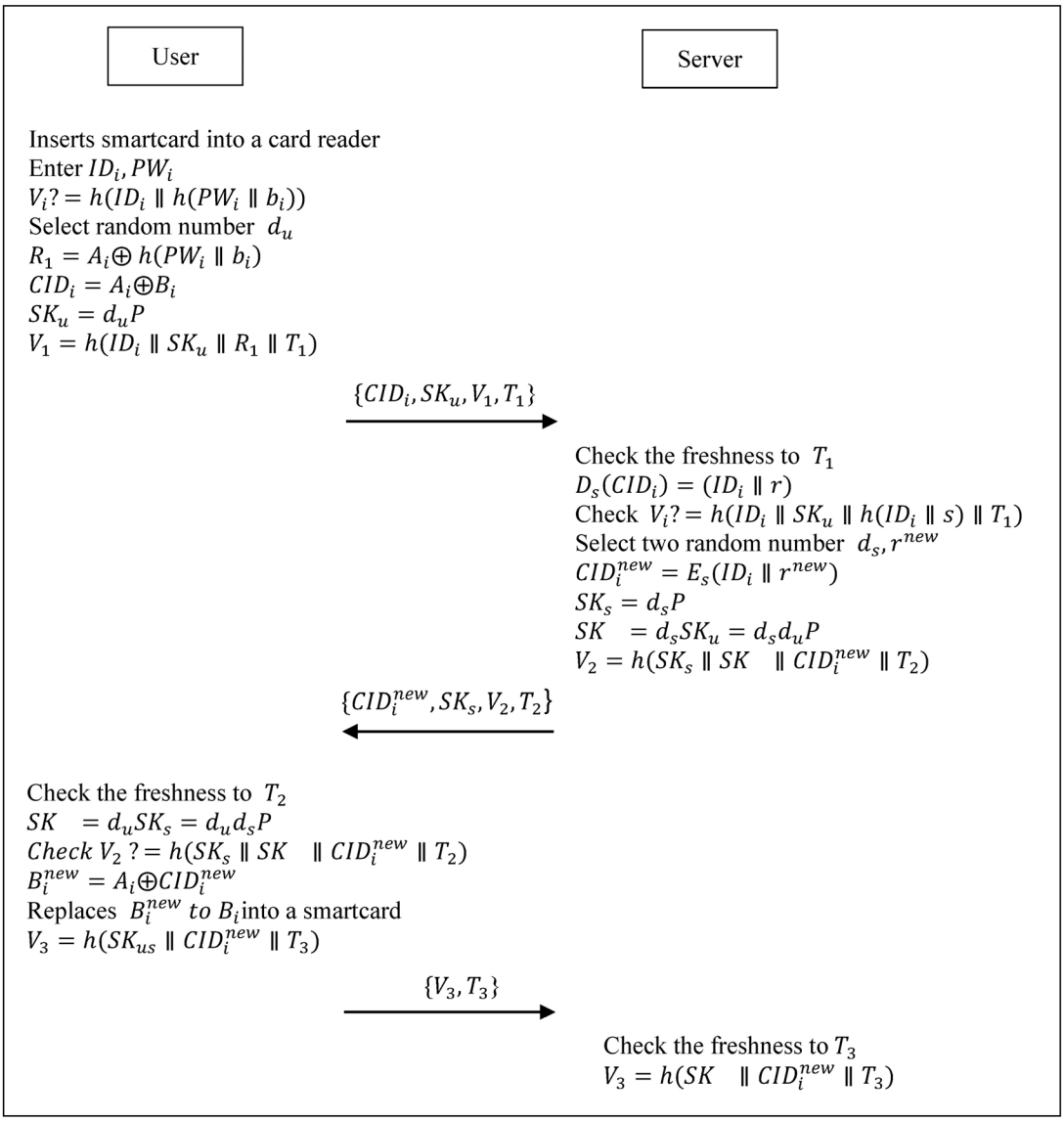

Figure 4. Login and verification phase of the proposed scheme

(1) The user inserts his/her smartcard into the card reader and enters his/her ID_i and PW_i. Then, a random number d_u is selected, and the reader system first verifies whether $h(ID_i \| h(PW_i \| b_i))$ equals V_i on the card; if not, the session terminated; if so, $R_1 = A_i \oplus h(PW_i \| b_i)$, $CID_i = A_i \oplus B_i$, $SK_u = d_u P$, and $V_1 = h(ID_i \| SK_u \| R_1 \| T_1)$ are calculated. Then, the login message $\{CID_i, SK_u, V_i, T_1\}$ is transmitted to the server through the public channel, where T_1 is the current timestamp.

(2) When the server receives the message $\{CID_i, SK_u, V_i, T_1\}$, it first checks the validity of the timestamp T_1. If it is within the validity, it calculates $D_s(CID_i) = (ID_i \| r)$ and verifies whether $h(ID_i \| SK_u \| h(ID_i \| s) \| T_1)$ equals V_i; if not, the session terminated; if so, it generates the random numbers d_s and r^{new} and calculates $CID_i^{new} = E_s(ID_i \| r^{new})$, $SK_s = d_s P$, $SK_{us} = d_s SK_u = d_s d_u P$, and $V_2 = h(SK_2 \| SK_{us} \| CID_i^{new} \| T_2)$. After the calculation, the message $\{CID_i^{new}, SK_s, V_2, T_2\}$ is sent to the user through the public channel, and T_2 is the current timestamp.

(3) When the user receives the message $\{CID_i^{new}, SK_s, V_2, T_2\}$, the server first checks the

validity of T_2. If it is within the validity, the server calculates $SK = d_u SK_s = d_u d_2 P$ and uses it to verify whether $h(SK_s \| SK \| CID_i^{new} \| T_2)$ equals V_2; if not, the session terminated; if so, $B_i^{new} = A_i \oplus CID_i^{new}$ and $V_3 = h(SK \| CID_i^{new} \| T_2)$ are calculated, and B_i in the smartcard is replaced with B_i^{new} ; then, $\{V_3, T_3\}$ is transmitted to the server through the public channel.

(4) After the server receives the message $\{V_3, T_3\}$, the server first checks the validity of T_3. If it is within the validity, the server verifies whether $h(SK \| CID_i^{new} \| T_3)$ equals V_3; if not, the session terminated; if so, the session key SK is accepted.

4.3 Password-changing Phase

If the user requirements to change the password, he/she should enter his/her account ID_i, the old password PW_i, and the new password PW_i^{new}. The steps at the user terminated are shown in Figure 5.

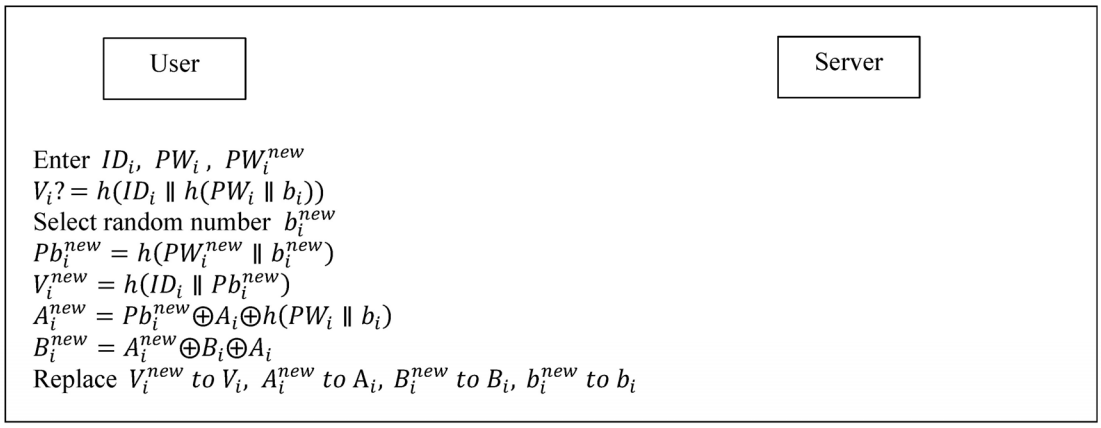

Figure 5. Password-changing phase of the proposed scheme

(1) Verify whether $h(ID_i \| h(PW_i \| b_i))$ is the same as V_i; if so, choose a random number b_i^{new} , and calculate $Pb_i^{new} = h(PW_i^{new} \| b_i^{new})$, $V_i^{new} = h(ID_i \| Pb_i^{new})$, $A_i^{new} = Pb_i^{new} \oplus A_i \oplus h(PW_i \| b_i)$ and $B_i^{new} = A_i^{new} \oplus B_i \oplus A_i$. After the calculation, V_i, A_i, B_i, and b_i in the smartcard are replaced with V_i^{new} , A_i^{new} , B_i^{new} and b_i^{new}

5 Security Analysis

This section explains that the proposed scheme can withstand insider, replay, offline password-guessing, and impersonation attacks and provides three features: perfect forward secrecy, user anonymity, and know-key security.

5.1 Insider Attacks

An insider attack means that, if there is an unscrupulous administrator, he/she can obtain member accounts and passwords.

At the login phase, the user transfers $Pb_i = h(PW_i \| b_i)$ to the server. Because the Hash function is unidirectional and b_i is a random number, an administrator cannot have password information from the hash values. Therefore, the proposed scheme can withstand Insider attacks.

5.2 Replay Attacks

Replay attack refers to an attacker using eavesdropping to record a previously transmitted authentication message, retransmitting it to the server, and logging in to the server by faking a legal user.

When the attacker resends the previous login message $\{CID_i, SK_u, V_1, T_1\}$ to the server, the server can check whether the T_1 timestamp is within the validity to judge whether it is a maliciously resent packet and can check if the message has been changed through the equation $V_i ? = h(ID_i \| SK_u \| h(ID_i \| s) \| T_1)$.

The attacker may also resend the server's return message $\{CID_i^{new}, SK_s, V_2, T_2\}$ to the user. The user can check whether the T_2 timestamp is within the validity to judge whether it is a resent packet and whether $V_2 ? = h(SK_s \| SK_{us} \| CID_i^{new} \| T_2)$ to see whether the message has been changed.

Therefore, the proposed scheme can resist replay attacks.

5.3 Offline Password-guessing Attacks

An offline password-guessing attack is guessing the correctness of a password using a stolen smartcard or a previously intercepted message.

Assuming that the attacker has stolen the user's smartcard $\{V_i, A_i, B_i, b_i, E, P, n, h(\ )\}$ and extracted A_i and B_i, as he/she does not know the key of the server s, he/she surely cannot extract the correct identity ID_i

and password PW_i from A_i and B_i. Therefore, the attacker cannot guess the password from the stolen smartcard message.

Because the password cannot be obtained from the smartcard, the attacker can only guess the password from the messages $\{CID_i, SK_u, V_1, T_1\}$ and $\{CID_i^{new}, SK_s, V_2, T_2\}$. In such messages, the information d_u contained in SK_u, d_s contained in SK_s, and the timestamps T_1 and T_2 are newly generated values, and CID_i is changed after each successful login. Therefore, all values are different for each message sent, and the attacker cannot distinguish which message is transmitted by which identity ID_i.

5.4 Impersonation Attacks

In impersonation attack, an attacker uses a user or server's authentication message and tries to impersonate one of them to defraud the other's information.

In the proposed scheme, an attacker only can extract the A_i and B_i from the smartcard and to calculate the $CID_i = A_i \oplus B_i$. Without the server private key s, the attacker cannot decrypt CID_i to obtain the user's real identity ID_i. Therefore, the verification message $V_1 = h(ID_i \| SK_u \| R_1 \| T_1)$ cannot be generated, so it is impossible to impersonate the user.

The attacker also cannot generate the server's return message $\{CID_i^{new}, SK_s, V_2, T_2\}$, because he/she does not know the server's private key s. Therefore, $CID_i^{new} = E_s(ID_i \| r^{new})$ and $V_2 = h(SK_s \| SK \| CID_i^{new} \| T_2)$ cannot be generated, so it is impossible to impersonate the server.

5.5 User Anonymity

User anonymity includes untraceability and protection of the user's real identity. In our scheme, the real identity ID_i is not transmitted via the public channel. When the attacker obtains the login request message $\{CID_i, SK_u, V_1, T_1\}$, the user's real identity ID_i still cannot be known, because $CID_i = E_s(ID_i \| r)$ is encrypted using the server's key s, while the attacker does not know the server's key s. Therefore, an attacker cannot obtain a real identity through a login request message. In addition, the new random number r^{new} and the new $CID_i^{new} = E_s(ID_i \| r^{new})$ are calculated each time the login information is verified, and, thus, the corresponding identity cannot be known from CID_i.

5.6 Perfect Forward Secrecy

Perfect forward secrecy refers to not knowing the previous message because the current message is cracked. In the proposed scheme, the session key calculated from the user and server is $SK = d_u\, d_s\, P$ where d_u and d_s are random numbers. If the attacker knows the server's secret key s or the user's identity ID_i and password PW_i, it cannot help the attacker to calculate the previous session key, because these messages are not used to calculate the session key. Even if the attacker obtains SK based on the difficulty of solving the elliptic curve discrete logarithm problem, neither d_uP nor d_sP can be derived based on the related information. Therefore, the proposed scheme provides perfect forward secrecy

5.7 Known-key Security

Known-key security means that the current session key will not be known because other session keys have been decrypted.

In the proposed scheme, if the attacker has stolen the session key $SK = d_u\, d_s\, P$ because d_u and d_s are random numbers, it is impossible to calculate other session keys from the current session key. Therefore, the proposed scheme provides know-key security.

6 Performance Analysis

We compared the proposed proposed scheme with those of Giri et al., Amin and Biswas, and Arshad and Rasoolzadegan. The results are shown in Table 3. To facilitate the evaluation of relevant computing costs, relevant symbols are defined in Table 2.

According to Jiang et al.'s scheme [8], the computing durations of exponential operation, elliptic curve point multiplication, symmetric encryption/ decryption, and hash function are 0.522s, 0.063075s, 0.0087s, and 0.0005s, respectively, and the computing duration of XOR can be ignored.

Table 2. Notations of symbols in performance analysis

Symbol	Description
T_E	Execute time of exponent operation
T_{PM}	Execute time of elliptic curve point multiplication
T_{SED}	Execute time of symmetric encryption/decryption
T_H	Execute time of hash function
T_X	Execute time of exclusive OR (XOR)

In the proposed scheme, the computing cost at the registration phase is $1T_{SED} + 3T_H + 2T_X$, which is equivalent to 10.2 milliseconds. The computing cost at the login and verification phase is $2T_{SED} + 4T_{PM} + 10T_H + 3T_X$, which is equivalent to 274.7 milliseconds. The computing cost at the password-changing phase is $4T_H + 3T_X$, which is equivalent to 2.5 milliseconds.

Table 3. Comparison between proposed scheme and other schemes

Comparison criteria			Schemes				
			Giri et al. [7]	Amin-Biswas [1]	Arshad-Rasoolzadegan [2]	Wu et al. [18]	Proposed Scheme
Computing cost	Registration Phase	Cost	$1T_E + 3T_H + 1T_X$	$5T_H + 3T_X$	$1T_{SED} + 3T_H + 1T_X$	$6T_H + 3T_X$	$1T_{SED} + 3T_H + 2AT_X$
		Time	523.5ms	2.5ms	10.2ms	3ms	10.2ms
	Login and verification Phase	Cost	$1T_E + 9T_H + 5T_X$	$2T_E + 15T_H + 7T_X$	$2T_{SED} + 4T_{PM} + 14T_H + 3T_X$	$4T_{PM} + 30T_H + 15T_X$	$2T_{SED} + 4T_{PM} + 10T_H + 3T_X$
		Time	526.5ms	1051.5ms	276.7ms	267.3ms	274.7ms
	Password-changing Phase	Cost	$1T_E + 5T_H + 2T_X$	$9T_H + 7T_X$	$2T_{SED} + 3T_{PM} + 13T_H + 5T_X$	$7T_H + 5T_X$	$5T_H + 3T_X$
		Time	524.5ms	4.5ms	213.125ms	3.5ms	2.5ms
Security properties	Resist password-guessing attacks		×	×	O	O	O
	Resist Replay attacks		×	×	O	O	O
	Resist Impersonation attacks		O	O	O	O	O
	Resist Insider attacks		×	O	O	O	O
	Provide Perfect forward secrecy		×	×	O	O	O
	Provide Mutual authentication		O	O	O	O	O
	Provide Know-key security		O	O	O	O	O
	Provide key agreement		O	O	O	O	O
	Protect User anonymity		×	O	O	O	O
	Change one's own password offline		O	O	×	×	O

Compared with other schemes, at the registration phase, the cost of the proposed scheme is higher than that of Amin and Biswas [1] and Wu et al. [18], roughly equal to that of Arshad and Rasoolzadegan [2], and lower than that of Giri et al. [7]. At the login and verification phase, the cost of the proposed scheme is lower than other most schemes except Wu et al.'s scheme. At the password-changing phase, the cost of the proposed scheme is the lowest one.

7 Conclusion

In this article, we found that Arshad-Rasoolzadegan's authentication scheme does not allow changing one's own password offline. To solve the problem and improve the efficiency, we proposed a new TMIS authentication scheme. Security analysis showed that we can resist all kinds of attacks and allow changing one's own password offline. According to the performance analysis, the proposed scheme has better performance than the previous schemes. Therefore, the authentication scheme we proposed is more suitable for TMIS.

References

[1] R. Amin, G. P. Biswas, An Improved RSA-based User Authentication and Session Key Agreement Protocol Usable in TMIS, *Journal of Medical Systems*, Vol. 39, No. 8, pp. 1-14, June, 2015.

[2] H. Arshad, A. Rasoolzadegan, Design of a Secure Authentication and Key Agreement Scheme Preserving User Privacy Usable in Telecare Medicine Information Systems, *Journal of Medical Systems*, Vol. 40, No. 11, pp. 237, November, 2016.

[3] T. Cao, J. Zhai, Improved Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems, *Journal of Medical Systems*, Vol. 37, No. 2, pp. 1-7, April, 2013.

[4] C. C. Chang, W. Y. Hsueh, T. F. Cheng, An Advanced Anonymous and Biometrics-based Multi-server Authentication Scheme Using Smartcards, *International Journal of Network Security*, Vol. 18, No. 6, pp. 1010-1021, November, 2016.

[5] H. M. Chen, J. W. Lo, C. K. Yeh, An Efficient and Secure Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems, *Journal of Medical Systems*, Vol. 36, No. 6, pp. 3907-3915, December, 2012.

[6] H. Debiao, C. Jianhua, Z. Rui, A More Secure Authentication Scheme for Telecare Medicine Information Systems, *Journal of Medical Systems*, Vol. 36, No. 3, pp. 1989-1995, June, 2012.

[7] D. Giri, T. Maitra, R. Amin, P. D. Srivastava, An Efficient and Robust RSA-based Remote User Authentication for Telecare Medical Information Systems, *Journal of Medical Systems*, Vol. 39, No. 1, pp. 145, January, 2015.

[8] Q. Jiang, J Ma, G. Li, L. Yang, An Efficient Ticket-based Authentication Protocol with Unlink Ability for Wireless Access Networks, *Wireless Personal Communications*, Vol. 77, No. 2, pp. 1489-1506, July, 2014.

[9] C. C. Lee, T. H. Lin, C. S. Tsai, A New Authenticated Group Key Agreement in a Mobile Environment, *Annals of Telecommunications- annales des télécommunications*, Vol. 64, No. 11, pp. 735-744, December, 2009

[10] C. T. Li, T. Y. Wu, C. L. Chen, C. C. Lee, C. M. Chen, An Efficient User Authentication and User Anonymity Scheme with Provably Security for IoT-based Medical Care System, *Sensors*, Vol. 17, No. 7, pp. 1-18, July, 2017.

[11] C. T. Li, C. Y. Weng, C. C. Lee, A Secure RFID Tag Authentication Protocol with Privacy Preserving in Telecare Medicine Information System, *Journal of Medical Systems*, Vol. 39, No. 8, article 77, pp. 1-8, Aug. 2015.

[12] C. T. Li, C. C. Lee, C. Y. Weng, C. I. Fa, An Extended Multi-Server-Based User Authentication and Key Agreement Scheme with User Anonymity, *KSII Transactions on Internet and Information Systems*, Vol. 7, No. 1, pp. 119-131, January, 2013.

[13] H. Y. Lin, On the Security of a Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems, *Journal of Medical Systems*, Vol. 37, No. 2, pp. 1-5, January, 2013.

[14] Y. J. Liu, C. C. Chang, S. C. Chang, An Efficient and Secure Smartcard-based Password Authentication Scheme, *International Journal of Network Security*, Vol. 19, No. 1, pp. 1-10, January, 2016.

[15] D. Mishra, *A Study on ID-based Authentication Schemes for Telecare Medical Information System*, http://arxiv.org/abs/1311.0151.

[16] R. Mishra, A. K. Barnwal, A Privacy Preserving Secure and Efficient Authentication Scheme for Telecare Medical information systems, *Journal of Medical Systems*, Vol. 39, No. 5, pp. 1-10, May, 2015.

[17] J. Wei, X. Hu, W. Liu, An Improved Authentication Scheme for Telecare Medicine Information Systems, *Journal of Medical Systems*, Vol. 36, No. 6, pp. 3597-3604, December, 2012.

[18] F. Wu, X. Li, L. Xu, S. Kumari, A.K. Sangaiah, A Novel Mutual Authentication Scheme with Formal Proof for Smart Healthcare Systems under Global Mobility Networks Notion, *Computers & Electrical Engineering*, Vol. 68, pp. 107-118, May, 2018.

[19] Z. Y. Wu, Y. C. Lee, F. Lai, H. C. Lee, Y Chung, A Secure Authentication Scheme for Telecare Medicine Information Systems, *Journal of Medical Systems,* Vol. 36, No. 3, pp. 1529-1535, June, 2012.

[20] Q. Xie, J. Zhang, N. Dong, Robust Anonymous Authentication Scheme for Telecare Medical Information Systems, *Journal of Medical Systems,* Vol. 37, No. 2, pp. 1-8, April, 2013.

[21] Z. Zhu, An Efficient Authentication Scheme for Telecare Medicine Information Systems, *Journal of Medical Systems,* Vol. 36, No. 6, pp. 3833-3838, December, 2012.

Biographies

Jung-Wen Lo received his PhD in Computer Science and Engineering from National Chung Hsing University, Taiwan. He is an associate professor in the Information Management Department of National Taichung University of Science and Technology, Taiwan. His research interests include network security, computer networks and IoT applications.

Chun-Yueh Wu has received his master degree in Department of Information Management from National Taichung University of Science and Technology, Taiwan, in 2019. His research is about telecare medicine information systems security. He is currently a PHP, Golang and C++ developer who focus on developing backend, frontend and software system.

Shu-Fen Chiou received her Ph.D. in Computer Science and Engineering from National Chung Hsing University, Taiwan in 2012. She is currently an assistant professor of Information Management at National Taichung University of Science and Technology, Taiwan. Her research interests include information security, network security, data hiding, and machine learning.