Journal of Medical Systems (2021) 45: 77
https://doi.org/10.1007/s10916-021-01750-7

MOBILE & WIRELESS HEALTH

Construction of a Chaotic Map-Based Authentication Protocol for TMIS

Dharminder Dharminder[1] · Nibedita Kundu[2] · Dheerendra Mishra[3]

Received: 1 September 2020 / Accepted: 10 June 2021 / Published online: 2 July 2021

Abstract

Upgraded network technology presents an advanced technological platform for telecare medicine information systems (TMIS) for patients. However, TMIS generally suffers various attacks since the information being shared through the insecure channel. Recently, many authentication techniques have been proposed relying on the chaotic map. However, many of these designs are not secure against the known attacks. In spite of the fact that some of the constructions attain low computation overhead, they cannot establish an anonymous communication and many of them fail to ensure forward secrecy. In this work, our aim is to present authentication and key agreement protocol for TMIS utilizing a chaotic map to achieve both security and efficiency. The underlying security assumptions are chaotic theory assumptions. This scheme supports forward secrecy and a secure session is established with just two messages of exchange. Moreover, we present a comparative analysis of related authentication techniques.

Keywords Healthcare systems · TMIS · Authentication and key agreement · Security · Anonymity

Introduction

The TMIS is applicable in various healthcare systems, such as remote user's medical monitoring, consultation, and health-related flexible and convenient services. In the healthcare sector, these systems are essential for the current demand as these provide private health facilities to the patients at their home. Healthcare services are improved due to the technological development in the network. As a consequence, electronic devices can be used by patients to receive healthcare services. We know that the users use the public insecure channel to access the service. This leads to a security threat. Thus, the communication must be through an effective authenticated channel in order to achieve privacy and security. To fill this gap, Wu et al. [10] came up with a secure authentication scheme for the system. In the following, Wei et al. [9] noticed that the work of Wu et al. [9] is vulnerable to two-factor authentication. Therefore, a new scheme is proposed based on a smart card for TMIS to validate two-factor authentication. In 2012, Zhu [12] found that in Wei et al.'s technique password guessing is possible. He proposed an advanced scheme, but that was without anonymous communication. Later, Chen et al. [5] developed an anonymous authentication technique for TMIS. In the following, Lin et al. [7] showed that in Chen et al.'s scheme, the user's identity can be disclosed with the help of the dictionary attack and guessing of the password is possible using smart card's information. In order to prevent the existing attacks, Lin et al. [7] presented an anonymous authentication scheme. Cao and Zhai [4] illustrated that the design of Chen et al. is vulnerable to password guessing and identity guessing attacks due to smart card information. Thus, they designed an efficient protocol for TMIS. The protocols [4, 7, 12] are not secure against input verifying conditions since incorrect input cannot be efficiently distinguished by these protocols. Cryptosystems, based on the chaotic maps, have been developed in order to improve efficiency and security. Apart from security, privacy attributes have equal importance. Two key privacy attributes are anonymity and

This article is part of the Topical Collection on *Mobile & Wireless Health*

✉ Dheerendra Mishra
dheerendra.m@gmail.com

[1] Department of Mathematics, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Chennai, India

[2] Department of Mathematics, The LNM Institute of Information Technology, Jaipur, India

[3] Department of Mathematics, Maulana Azad National Institute of Technology, Bhopal, India

unlinkability, which are missing in many authentication schemes for TMIS, such as [9, 10, 12, 31] protect user's anonymity. In 2013, Guo et al. [14] constructed an AKA-CM (authenticated Key agreement based on the chaotic map) protocol. Later, Hao et al. [15] showed that the work [14] does not provide the user traceability due to the use of two secret keys. Hoa et al. then developed a new technique that performs better over the work of Guo et al. In 2014, the weaknesses in Hoa et al.'s scheme were noticed by Jiang et al. [16]. They observed that the scheme is not secure against the stolen smart card (SSC) attack. Li et al. [21], in 2016, proposed an AKA-CM for healthcare. However, Madhusudhan et al. noticed that the design is vulnerable to impersonation (IMP) and password guessing (PAG) attacks. Later, Jiang et al. [27] presented an improved AKA model for TMIS, which uses three messages of exchange for session key agreement. Moreover, this scheme is not much efficient as it uses six elliptic curve scalar multiplication as given in [27], which has the highest cost as given in [27]. At the same time, Wu et al. [28] presented RFID based AKA scheme, which uses the hash function. In the following, Radhakrishnan et al. [19] presented an authentication protocol (AUTP) for TMIS which is not secure against identity guessing (IDG), SSC information, and PAG attacks. Later, Zhang et al. [25] proposed an AUT (authentication technique) for TMIS. Unfortunately, this protocol is also insecure against PAG, IDG, and replay (RPL) attacks. In the following, a robust AUT was developed by Madhusudhan et al. [20] for telecare medical information system (TMIS). However, it can be observed that their scheme remains insecure against SSC, IMP, PAG, and IDG attacks. The brief analysis of security attributes is given in Tables 1 and 2. In [34], Li et al. presented a cloud-assisted mutual authentication and privacy preservation protocol for TIMS. In the following, a secure mutual authentication protocol for cloud-assisted TMIS based on elliptic curve cryptography was proposed by Kumar et al. [35]. Later on, Salem and Amin [36] developed an RFID authentication protocol relying on El-Gamal cryptosystem for secure telecare medical information systems. Nayak and Pippal [38] also discussed existing authentication protocols for TMIS and did their efficiency analysis. Recently, a chaotic hash function based lightweight client authentication scheme with anonymity for TMIS was proposed by Gaikwad et al. [37].

As we know $T_h \approx 0.00032s$ is a very light weight operation as we compared with other's such as $t_{me} \approx 0.0192s$, $t_{fe} \approx t_{h_b} \approx t_{ecm} \approx 0.0171s$ [32], $t_b \approx 0.380s$, $t_{sym} \approx 0.0056s$, $t_{ecm} \approx t_c \approx 0.0171s$ [2]. We compare the performance of related schemes in. Figure 1.

A comparative summary of the security attributes of authentication protocols (chaotic map-based) for TMIS is given in Table 2. We use the notations $\surd$ and $\times$ to denote that a scheme achieves the attribute and fails to attain the attribute respectively. It can be seen from Tables 1 and 2 that existing protocols for TMIS are weak from a security point of view. In other words, the protocols cannot resist all existing attacks as provided in Tables 2 and 1. Thus, it is required to have an AKA-MP for TMIS preserving the following attributes:

- User friendly login and password update.
- Unlinkability.
- Mutual authenticated secure session-key based Communication.
- Low computational overhead and high security.
- Less communication overhead and anonymity.

Therefore, we proposed a secure and efficient AKA-MP for TMIS. The security analysis of our scheme is given in this work. Our construction is resistant to existing attacks and possesses a key agreement using two message exchange.

Roadmap

The paper is originated as follows: Basic assumptions, notations and model is discussed in "Preliminaries". The proposed scheme is described in "Proposed Scheme". The claim of security is proved in "Security Analysis". The performance of the proposed scheme is discussed in "Computational Efficiency Analysis". Lastly, conclusion is provided in "Conclusion".

Table 1 Key attributes comparison of password based AUTP for TMIS

Security attributes\Schemes	[5]	[4]	[11]	[7]	[29]	[24]	[13]	[30]
User anonymity (UAN)	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\times$
Off-line PAG	$\times$	$\times$	$\times$	$\surd$	$\surd$	$\surd$	$\times$	$\times$
SSC	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$
User IMP	$\times$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\times$	$\surd$
Replay	$\surd$	$\times$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$
Linkability	$\times$	$\surd$	$\surd$	$\surd$	$\surd$	$\times$	$\times$	$\times$
Session-key agreement (SKA)	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$
Session-key verification (SKV)	$\times$	$\surd$	$\times$	$\times$	$\times$	$\surd$	$\times$	$\times$

Table 2 Key attribute comparison of AKA-CM for TMIS

Security attributes/Schemes	[24]	[15]	[22]	[23]	[25]	[19]	[21]	[20]
Insider	√	√	√	√	√	√	√	√
Linkability	×	√	√	√	√	×	√	×
Offline PAG	√	√	√	√	×	×	×	×
SSC	√	√	√	√	√	×	√	×
Server IMP	√	√	√	√	√	√	×	×
Use IMP	√	√	√	√	√	√	×	×
Replay	√	√	√	√	×	√	√	√
UAN	√	√	×	√	×	×	×	×
SKV	√	×	√	×	√	√	×	√
SKA	√	√	√	√	√	√	√	√

Preliminaries

The notations and basic definitions are presented in this section. Also Chaos theory's definition with its properties are discussed. The description of the notations is given as in Table 3.

Chebyshev Chaotic Map (CCM)

The following definition of CCM are taken from [17, 18].

- **Definition 1** Chebyshev polynomial (CHP) of degree n (positive integer) is denoted by $T_n(x)$ and defined as $T_n(x) = cos(n(\arccos(x)))$ such that $T_n(x) : (-\infty, +\infty) \rightarrow [-1, +1]$. It satisfies the relation $T_n(x) = (2xT_{n-1}(x) - T_{n-2}(x))$ for $x \in (-\infty, +\infty)$, $T_0(x) = 1$ and $T_1(x) = x$
- **Definition 2** The DLP (discrete logarithm problem) is to compute an integer u satisfying the equality $T_u(x) = y$ given y and x.
- **Definition 3** Computational Diffie-Hellman (CDH) problem is defined as follows: given the tuple $(x, T_u(x), T_v(x))$, it is hard to compute $T_{uv}(x)$.

Threat model

We follow the notations as described in Table 3 and a threat model as depicted in Figure (1) under security assumptions [8] about the computational power of $\Re$ in smart card security in password-based and chaotic map-based authentication schemes.

- The pseudo-random password is chosen by the user from the dictionary. S_j has private key. Essential values are inserted by the server in the smart card during the registration.
- The $\Re$, U_i and S_j communicate via oracle queries that enable $\Re$ to break authentication scheme.
- The $\Re$ controls the communication channel by intercepting, modifying, resenting and diverting the message.

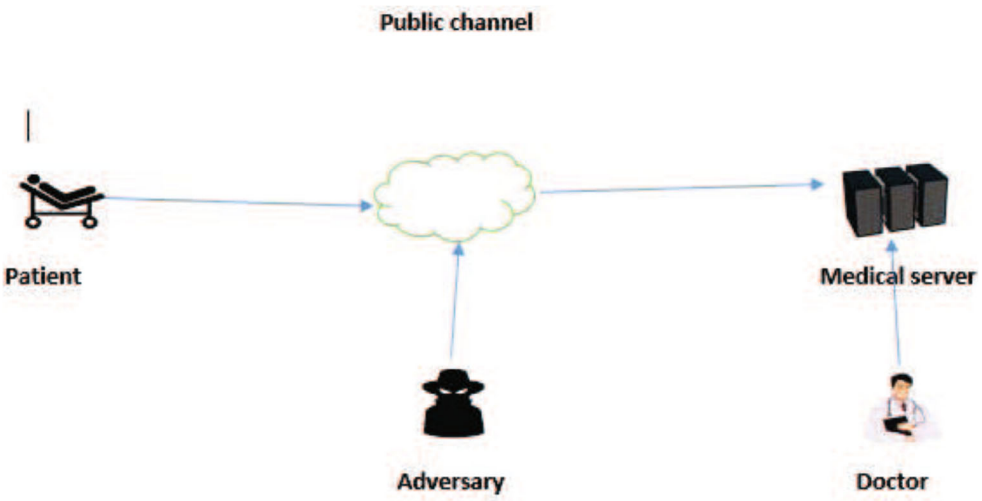

Fig. 1 Computational cost comparison of related schemes

Table 3 Notations

Description	Notation
User-i	U_i
Server-j	S_j
Adversary	$\Re$
Smart Card	Sc
Identity of U_i	Id_i
Password of U_i	Pw_i
Secret value of S_j	x
Hash	$h(\cdot)$
Biometric hash	$h_b(\cdot)$
Telecare medicine information system	$TMIS$
Bitwise XOR	$\oplus$
String concatenation	$\|\|$

- The $\Re$ can steal the smart card and can get its stored information.

Proposed Scheme

We now present an AKA-CM to address the security and efficiency requirements.

Registration Phase

U_i adopts secure channel to complete his registration with S_j. The communication of messages and computation are described in Fig. 2.

- U_i chooses Id_i, Pw_i,imprints biometric $H_i = h_b(biometric)$ and executes $A_i = h(Id_i||Pw_i||H_i)$ and forwards $\{Id_i, A_i\}$ to S_j.
- The S_j, after recovering $\{Id_i, A_i\}$, checks the correctness of U_i's identity Id_i. If validation succeeds, then S_j uses its secret key x to derive $T_x(Id_i||n_i)$ for user U_i, where $n_i \in Z_p^*$ is randomly chosen. Sc then derives $B_i = T_x(Id_i||n_i) \oplus A_i$.
- Using secure channel, S_j issues Sc storing $\{h(.), B_i, n_i\}$ to U_i. S_j stores n_i corresponding to Id_i in secure database.
- U_i then puts in D_i in Sc along-with $\{h(.), B_i, D_i, n_i\}$ after computing $T_x(Id_i||n_i) = B_i \oplus A_i, D_i = h(T_x(Id_i||n_i)||Pw_i||Id_i||H_i)$.

Login Phase

U_i login to S_j by following steps. Description is provided via Fig. 3.

- U_i inserts Sc, Id_i and Pw_i. U_i imprints his biometric on sensor and computes $H_i' = h_b(biometric)$ and $A_i' = h(Id_i||Pw_i||H_i)$.
- Utilizing A_i', Sc receives $T_x(Id_i||n_i)' = A_i' \oplus B_i$ and executes $D_i' = h(T_x(Id_i||n_i)'||Pw_i||Id_i||H_i)$ and verifies the equality $D_i' \stackrel{?}{=} D_i$. The verification holds if all input parameters Id_i, Pw_i and biometric are correct.
- Sc chooses $y \in Z_p^*$ randomly and derives $W_i = T_y T_x(Id_i||n_i)$, $C_i = T_y(Id_i||n_i)$, $G_i = Id_i \oplus h(T_y(Id_i||n_i)||W_i||T_1)$ and $F_i = h(T_x(Id_i||n_i)||W_i||T_1)$. Finally, U_i transmits $\{C_i, G_i, F_i, T_1\}$ to S_j.

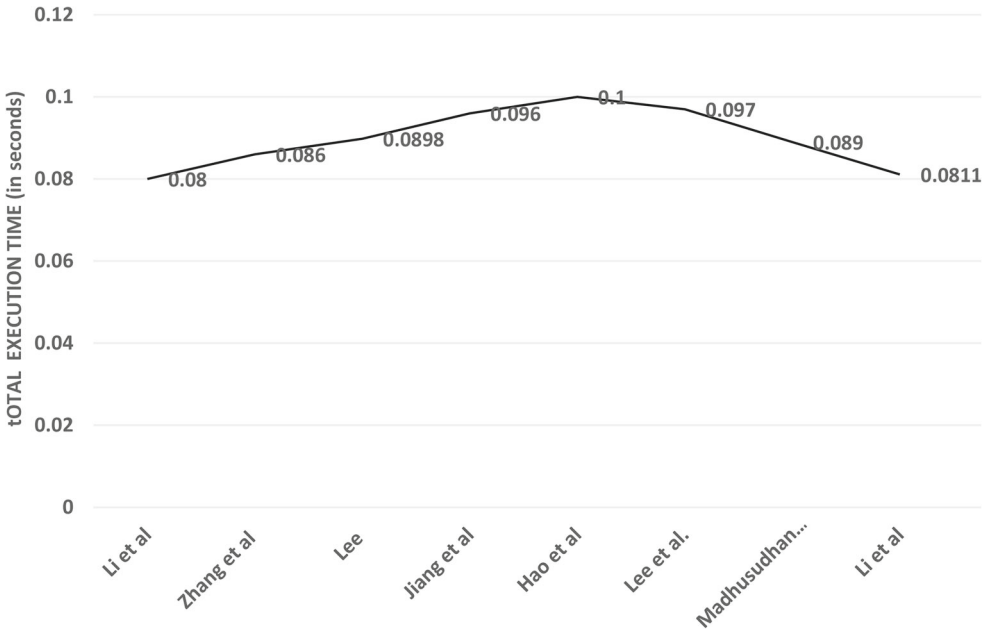

Fig. 2 Communication model

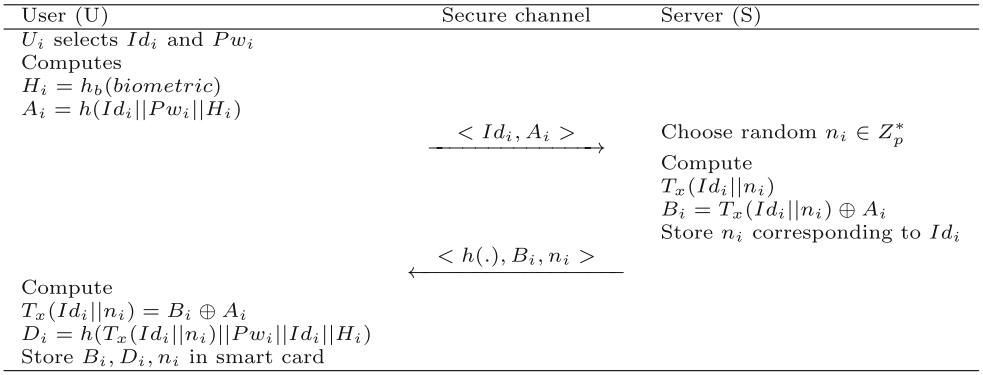

Fig. 3 Registration through secure channel

Authentication Phase

Description is provided via Fig. 4. On receiving $\{C_i, F_i, T_1\}$ from U_i, S_j performs the following steps:

- S_j verifies correctness of T_1, and then derives $T_xT_y(Id_i||n_i) = W_i'$, $Id_i = G_i \oplus h(T_y(Id_i||n_i)||Sk_i'||T_1)$ and $F_i' = h(T_x(Id_i||n_i)||Sk_i'||T_1)$, and verifies the equality $F_i' \stackrel{?}{=} F_i$ to check user validity.
- S_j selects a random value z and computes $C_j = T_z(Id_i||n_i)$, $W_j = T_zT_y(Id_i||n_i)$, $Sk_j = h(W_i'||W_j||T_1)$ and $F_j = h(Sk_j||W_j||T_2)$.
- S_j transmits $\{F_j, C_j, T_2\}$.
- On receiving $\{F_j, C_j, T_2\}$, U_i verifies the correctness of T_2, then executes $W_j' = T_zT_y(Id_i||n_i)$, $Sk_i = h(W_i||W_j'||T_1)$ and $F_j' = h(Sk_i||W_j'||T_2)$ and verifies $F_j' \stackrel{?}{=} F_j$. If verification succeeds, U_i accepts $Sk_i = h(W_i||W_j'||T_1)$.

Security Analysis

Our construction achieves mutual authentication and makes a secure communication between the U_i and the S_j.

Description of Existing Attacks

Our protocol is secure against insider attack, offline PAG attack, online PAG attack, server IMP attack and the user IMP attack, which are described below:

Three factor authentication: U_i with valid smart cart can execute the login session only after successfully delivering three factors $\{Id_i, Pw_i, H_i\}$ as session executes after the verification of $D_i \stackrel{?}{=} h(X_i||Pw_i||Id_i||H_i)$, where $H_i = h_b(biometric)$ and $X_i = h(Id_i||Pw_i||H_i) \oplus B_i$. In order to get $X_i = T_x(Id_i||n_i)'$, $\Re$ requires three factors $\{Id_i, Pw_i, H_i\}$ as $X_i = A_i \oplus B_i$, where $A_i' = h(Id_i||Pw_i||H_i)$. The two factors $(pw_i,\ biometric)$ are only with U_i. The Third factor (Id_i) masked value (G_i) is transmitted, where $G_i = Id_i \oplus h(T_y(Id_i||n_i)||W_i||T_1)$. To extract, Id_i from G_i, $\Re$ has to calculate $W_i = T_yT_x(Id_i||n_i)$, which is computationally infeasible.

Anonymity and unlinkability: Dynamic value (masked identity) G_i instead of Id_i is involved in the message transmission, i.e. $\{C_i, G_i, F_i, T_1\}$. Moreover, it is computationally infeasible to achieve Id_i using G_i and $T_y(Id_i||n_i)$ as $G_i = Id_i \oplus h(T_y(Id_i||n_i)||W_i||T_1)$, where $W_i = T_yT_x(Id_i||n_i)$. It justifies that protocol ensures anonymity.

Furthermore, linking of any two sessions messages is not possible in proposed protocol as all the values of transmitted messages $\{C_i, G_i, F_i, T_1\}$ and $\{F_j, C_j, T_2\}$ calculated using randomly generated values or timestamp. In other words, since during communication $T_y(Id_i||n_i)$, $T_z(Id_i||n_i)$, T_1 and T_2 changes every time, the proposed protocol supports unlinkability. Hence anonymity and unlinkability is preserved.

Insider attack: It is a form of malicious attack performed on a computer or network by entity who is having authorized system access. In our scheme, it is impossible to get a U_i's password by any destructive insider in the system. U_i submits the masked value of password as $h(Id_i|Pw_i||H_i)$ instead of Pw_i to S_j, where $h(.)$ is considered secure one way function. Thus, due to this secure hash function, any insider is unable to retrieve the password Pw_i of the user. Moreover, $\Re$ cannot guess the password as to guess the password, $\Re$ needs $H_i = h_b(biometric)$.

Stolen smart card attack: This attack fails as $\Re$ is unable to extract the value $T_x(Id_i||n_i)$, which is required to initiate login session. As $T_x(Id_i||n_i) = A_i \oplus B_i$ and $A_i = h(Id_i||Pw_i||H_i)$, thus to get $T_x(Id_i||n_i)$ $\Re$ has to compute $A_i = h(Id_i||Pw_i||H_i)$. The computation of $A_i = h(Id_i||Pw_i||H_i)$ requires three factors $\{Id_i, Pw_i, H_i\}$, which are only with U_i. Moreover, neither A_i nor any factor $\{Id_i, Pw_i, H_i\}$ are

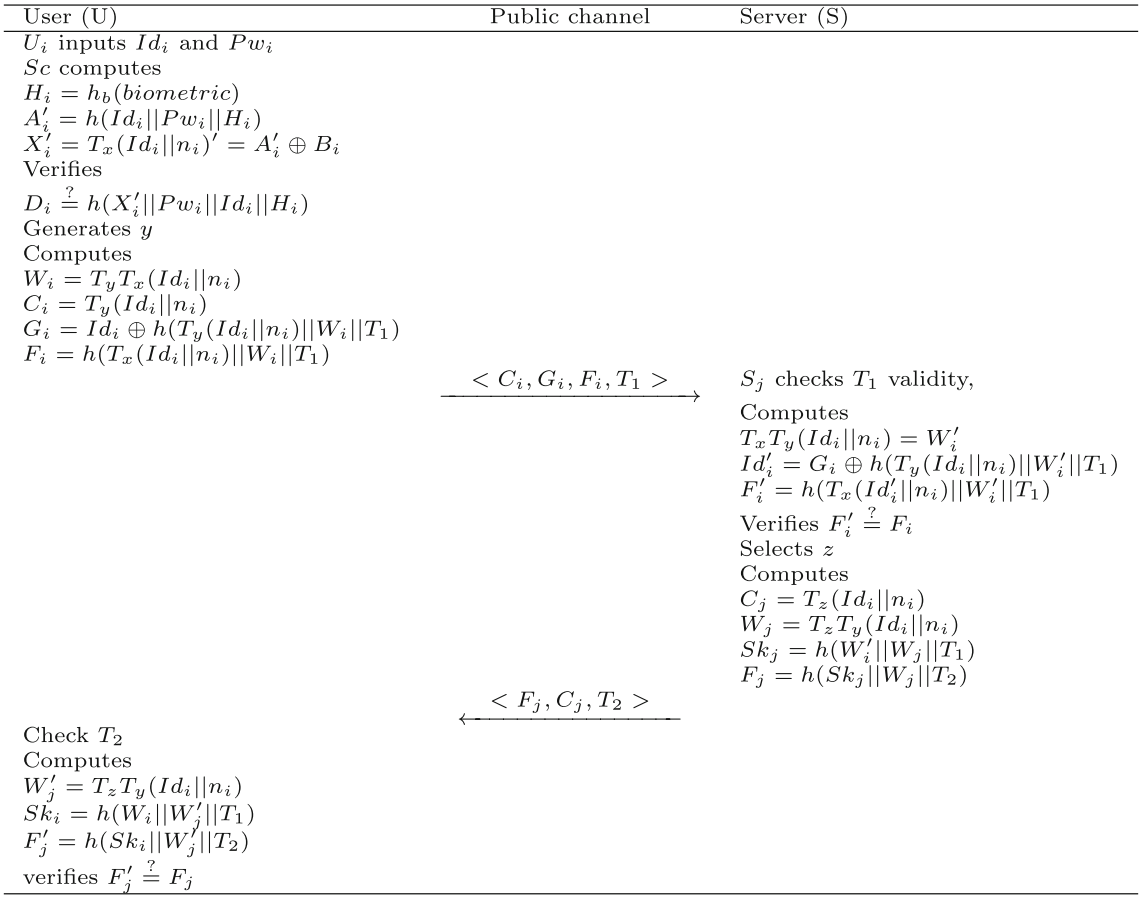

Fig. 4 Illustration of login and authentication via open channel

stored in Sc. To directly compute $< T_x(Id_i||n_i) >$, S_j secret key x and user's Id_i are required. However, both parameters (x, Id_i) are not public.

Off-line password guessing attack: To verify the guessed password, $\Re$ can use the condition $D_i \stackrel{?}{=} h(X_i||Pw_i||Id_i||H_i)$. However, the computation of D_i requires the knowledge of the secret factors $\{Id_i, Pw_i, H_i, X_i\}$, where $H_i = h_b(biometric)$, $X_i = A_i \oplus B_i$, $A'_i = h(Id_i||Pw_i||H_i)$. To compute X_i from B_i, $\{Id_i, H_i\}$ are needed other then guessed Pw_i. Since both the factors (Id_i, H_i), are unknown to $\Re$, it cannot correctly guess Pw_i.

Replay attack: This attack is a kind of network attack where transmission of valid data is maliciously delayed or repeated by an originator or by an advisory who intercepts the data and retransmits it. In our scheme, $\Re$ can retrieves the old transmitted messages $\{C_i, G_i, F_i, T_1\}$ and $\{F_j, C_j, T_2\}$ as these messages transmits via public channel. However, S_j and U_i can easily verify the replay of old messages using timestamp.

User impersonation attack: $\Re$ can retrieves the messages $\{C_i, G_i, F_i, T_1\}$ and $\{F_j, C_j, T_2\}$ as these messages transmits via public channel. However, to establish a valid session $\Re$ has to compute the fresh login message as proposed scheme resist replay attack. $\Re$ cannot modify the previously transmitted message $\{C_i, G_i, F_i, T_1\}$ to impersonate as $\Re$ has to update $F_i = h(T_x(Id_i||n_i)||W_i||T_1)$, which is not possible as this is the output of hash function and to freshly compute F_i, $T_x(Id_i||n_i)$ is needed. Moreover, $\Re$ can also get the values $\{B_i, D_i, n_i\}$ from the lost/ stolen card. However, this information is also not sufficient to impersonate a valid user, which is shown in stolen smart card attack.

Server impersonation attack: The $\Re$, with the knowledge of $\{h(.), B_i, D_i, n_i\}$ and old transmitted messages $\{C_i, G_i, F_i, T_1\}$ and $\{F_j, C_j, T_2\}$, cannot impersonate a server as follows:

(a) U_i can easily detect old transmitted message $\{F_j, C_j, T_2\}$ using timestamp T_2 and $F_j = h(Sk_j||W_j||T_2)$, where $W_j = T_z T_y(Id_i||n_i)$, $Sk_j = h(W_i||W_j||T_1)$ and $W_i = T_y T_x(Id_i||n_i)$.

(b) $\Re$ cannot generate fresh response by impersonating server as $\Re$ has to compute $F_j = h(Sk_j||W_j||T_2)$, which requires the information of S_j or U_i secret key.

Forward secrecy: With the knowledge of S_j's secret key x, $\Re$ cannot compute $Sk_i = h(W_i||W_j'||T_1)$ as

(a) Session key is defined as $h(W_i||W_j||T_1)$.
(b) Computation of Sk_i requires, the computation of W_i and W_j, where $W_i = T_yT_x(Id_i||n_i)$ and $W_j = T_zT_y(Id_i||n_i)$.
(c) Computation $W_j = T_zT_y(Id_i||n_i)$ using $T_y(Id_i||n_i)$ and $T_z(Id_i||n_i)$ is infeasible.
(d) Without the knowledge of W_j, $\Re$ cannot compute Sk_i.

Proof of Security

In this section, the security of our proposed scheme is explained against the general attacks. Here, we follow the symbols of [6].

(a) Existential-UNT-QSE (E-UNT-QSE): Here, the $\Re$ is not successful to choose request format of the user by communicating with the server and the smart card. In addition to that, he would not be able to eavesdrop over the existing channel.
(b) Forward-UNT-QSER (F-UNT-QSER): Here, the $\Re$ would not be able to trace past information on receiving the smart card which leaks stored information.

The following channels are to be used for oracles in our proof:

- **CHA1:** Transmitting messages to the S_j from the U_i .
- **CHA2:** Transmitting messages to the U_i from the S_j.

The following oracles will be used in our proof:

- **Query**(π_U^i, m_1, π_S^j) A request m_1 is sent to the server by $\Re$ via CHA1.
- **Send**$(\pi_{S_j}^k, m_2, \pi_U^i)$**:** On receiving the query in CHA2, m_2 is sent to the server by $\Re$ via CHA2 in order to obtain the S_j's access.
- **Execute**(π_U^i, π_S^j)**:** $\Re$ uses an instance of the protocol P run between S_j and smart card, and retrieves the messages which are communicated via CHA1, CHA2.
- **Reveal** (π_U^i): $\Re$ obtains the stored information in the smart card of the user. This may be utilized once so that Query (Q), Send (S), Execute (E) and Reveal (R) may not be applied further.

Theorem 1 *The proposed key agreement protocol P is E-UNT-QSE.*

Proof Let us assume that $\Re$ has taken $\mathcal{Q}$-Oracle so that $\omega_i(U_1) \in \{Query(\pi_{U_1}^i, *)\}$ and $\omega_i(U_2) \in \{Query(\pi_{U_2}^i, *)\}$. The output $m_1 \in \langle C_i, F_i, T_1\rangle$ of $\mathcal{Q}$-Oracle and simultaneously $m_2 \in \langle C_j, T_i\rangle$, F_i of the S_j are unlinkable due to the dynamic parameter $F_i = h(T_x(Id_i||n_i)||W_i||T_1)$. To retrieve Id_i, $\Re$ has to find y from $T_y(Id_i||n_i)$ which is chaotic based discrete logarithm problem. Since, DLP problem is computationally hard, $\Re$ cannot get Id_i from F_i and $T_y(Id_i||n_i)$. Additionally, $F_i = h(T_x(Id_i||n_i)||W_i||T_1)$ is generated using random number y as $W_i = T_yT_x(Id_i||n_i)$. For different sessions this changes F_i, which is essential. During communication also the time-stamp T_1 changes. Therefore, it is impossible to link the communicated messages. The S_j sends H_i after inserting T_2. $C_j = T_z(Id_i||n_i)$ is clearly dynamic. Here, the value Id_i is masked with the dynamic value so that in each session the output is changing. Hence, the proposed scheme offers anonymity along with unlinkability in the communication between U_i and S_j.

In $CHA1$, the U_i cannot be impersonated by $\Re$ since he has no knowledge about Pw_i, Id_i and the private key x of S_j. In a similar manner, the S_j cannot be impersonated by $\Re$ in $CHA2$ as he has no knowledge about S_j's secret key x and the user's Id_i. Hence, our scheme stops unauthorized U_i and S_j to impersonate in $CHA1$ and $CHA2$. Thus, in the given $\mathcal{Q}$-Oracle, the $\Re$'s advantage is not important as he gets no useful information. Therefore, P is E-UNT-Q. Assume that $\Re$ gets QS-Oracle's access such that $\omega_i(U_1) \in \{Query(\pi_{U_1}^i, *), Send(*, \pi_{U_1}^i)\}$ and $\omega_i(U_2) \in \{Query(\pi_{U_2}^i, *), Send(*, \pi_{U_2}^i)\}$. The S_j will not be impersonated by $\Re$ he has no knowledge of Id_i, y and the S_j's secrete key. Therefore, $\Re$ has trivial advantage with the $\mathcal{QS}$-Oracle's help. So, P is E-UNT-QS. Let us consider that the $\Re$ has $\mathcal{QSE}$-Oracle's access such that $\omega_i(U_1) \in \{Query(\pi_{U_1}^i, *), Send(*, \pi_{U_1}^i), Execute(\pi_{U_1}^i, \pi_S^j)\}$ and $\omega_i(U_2) \in \{Query(\pi_{U_2}^i, *), Send(*, \pi_{U_2}^i), Execute(\pi_{U_2}^i, \pi_S^j\}$. Due to the fresh use of y, T_1, T_2, the messages exchanged during P's execution are unique. Moreover, the replay of an old is stopped by the timestamp. Any old message cannot be used further as the S_j verifies a masked message and the $\Re$ has no knowledge of the server's private key x and the random number y. Hence, P is E-UNT-QSE which is the necessary security feature. □

Theorem 2 *Our key agreement protocol P is resistant to active-attacks.*

Proof Suppose $\Re$ gets $\mathcal{QSE}$-Oracle's access and in all the session, during communication he modifies the message. If the S_j or the U_j believe that a modified message is correct then the protocol is not secure against an active attack. In this case, our goal is to prove that the $\Re$ has a trivial

advantage. Suppose, the $\Re$ uses the $\mathcal{Q}$-Oracle to change a message in the CHA1 and simultaneously in the CHA2. But, the modified message cannot be accepted in the S_j and U_i as the S_j verifies T_i, the F_i and the Id_i in M_1 during authentication phase. Moreover, H_i in M_1 is verified by the user during the authentication phase.

If the $\Re$ uses the $\mathcal{Q}$-Oracle to change a message $\{C_i, F_i, T_1\}$ of communication, the S_j verification becomes invalid in $F_i = h(T_x(Id_i||n_i)||W_i||T_1)$.

Due to the chaotic discrete logarithm problem and the hash function, the $\Re$ cannot modify the message. Furthermore, he uses the $\mathcal{QS}$-Oracle to modify a message in the CHA2. Therefore, $\Re$ will get a trivial advantage because the U_i checks the C_j, T_2. Moreover, even if the $\Re$ has $\mathcal{QSE}$-Oracle's access, then also he would not be able to get success by performing the communication repeatedly. The verification of the modified message is not possible and in the concerned communication, the authorized entity terminates the session key. Hence, P is secure against active attacks. □

Analysis of Security using BAN Logic

BAN logic [26] is a set of rules for analyzing message exchange protocols. BAN logic assumes that the information exchange happens public monitoring.For verification following notations used:

1. $A| \equiv Y$: The principal A acts as Y holds.
2. $A \triangleleft Y$: An entity sent Y to A who can read and repeat Y.
3. $A| \sim Y$: A once said Y, implies $A| \equiv Y$ when A sent it.
4. $A| \Rightarrow Y$: A controls Y, A has an jurisdiction on Y .
5. $\#Y$: Message Y is fresh means Y never sent before.
6. $A| \equiv B \overset{k}{\longleftrightarrow} A$: A and B use K common shared key for communication.
7. $A \overset{K}{\rightleftharpoons} B$: secret K is used by A and B.
8. $\{Y\}_k$: The Y is encrypted with k.
9. $< Y >_X$: The formula Y is blended with formula X.
10. $(Y)_k$: The Y formula is keyed hash with the k.

For description of BAN logic terms [26], the required rules are discussed below:

Rule (1) Message means rule care of messages:

For shared private keys:

$$\frac{A| \equiv B \overset{k}{\longleftrightarrow} A, A \triangleleft \{X\}_k}{A| \equiv B \sim X} \tag{1}$$

If A trusts that B knows k and looks X encrypted with k, A trusts that B once said X.

Rule (2) The nonce verification rule confirms message is recent:

$$\frac{A| \equiv \#(X), A| \equiv B| \sim X}{A| \equiv B| \equiv X} \tag{2}$$

If A trusts that X is fresh and A trusts that B once said X, A trust that B believes X.

Rule (3) The jurisdiction rule ensures that A trusts B has jurisdiction on X:

$$\frac{A| \equiv B| \equiv X, A| \equiv B| \Rightarrow X}{A| \equiv X} \tag{3}$$

Rule (4) The freshness rule ensures that message is true if one part of message is true:

$$\frac{A| \equiv \#(X)}{A| \equiv \#(X, Y)} \tag{4}$$

According to the BAN logic, the presented scheme achieves: Goal 1. $U_i| \equiv (U_i \overset{Sk}{\longleftrightarrow} S_j)$; Goal 2. $S_j| \equiv (U_i \overset{Sk}{\longleftrightarrow} S_j)$; The protocol type:

Message 1. $U_i \rightarrow S_j : C_i = T_y(Id_i||n_i), F_i = h(T_x(Id_i||n_i)||W_i||T_1), T_1$.

Message 2. $S_j \rightarrow U_i : C_j, T_2$ We assume the following about the initial condition of the protocol to analyze given protocol:

A1: $U_i| \equiv \#(T_1)$; A2: $S_j| \equiv \#(T_2)$; A3: $U_i| \equiv (U \overset{X_U}{\longleftrightarrow} S)$; A4: $S_j| \equiv (U \overset{X_U}{\longleftrightarrow} S)$; A5: $U_i| \equiv S| \equiv (U \overset{X_U)}{\longleftrightarrow} S)$; A6: $S_j| \equiv U| \equiv (U \overset{X_U}{\longleftrightarrow} S)$; We analyze proposed protocol based on the BAN logic and the proof of presented scheme is given as follows:

With the message 1, we obtain goal (2):

S_1: $S \triangleleft (ID_{U_i}, T_{u_i}(y), T_1)_{x_u}, T_{u_i}(y).T_1$

According to A4, we apply the rule :

S_2: $S| \equiv U| \sim T_1$

According to the A1, we apply the freshness rule to get:

S_3: $S| \equiv \#(ID_{u_i}, T_{u_i}(x), T_1)_{X_u}$

With the S_2 and S_3, apply the nonce verification

S_4: $S| \equiv U| \equiv (T_{u_i}(y), T_1)_{X_u}$

According to the A4 and S_4, we concern the jurisdiction to get:

S_5: $S| \equiv T_1$

According to $sk = h(T_yT_x(Id_i||n_i)||T_zT_y(Id_i||n_i)||T_1)$, S_5 and A2, we could obtain

S_6: $S| \equiv (U \overset{Sk}{\longleftrightarrow} S)$ With the message 2, we could achieve goal (1):

S_7: $U \triangleleft (ID_{u_i}, T_1, T_2)_{X_U}, T_2$

With the assumption A3 and the message meaning rule we get:

S_8: $U| \equiv S| \sim T_2$

With the A2, we apply the freshness rule and get:

Table 4 Comparison of proposed scheme with the related authentication schemes

Schemes	User side operations	Server side operations	No of messages
Wu et al.'s [3]	$t_h + t_b + 3t_{ecm} + t_{sym}$	$4t_h + 4t_{ecm} + t_{sym}$	3
Wang et al.'s [1]	$2t_h + 3t_{ecm} + t_b$	$t_b + 3t_{ecm} + 2t_h + t_{me}$	2
Madhusudhan et al's [20]	$10t_h + 3t_c$	$6t_h + 2t_c$	2
Li et al.'s [21]	$6t_h + 3t_c$	$3t_h + 1t_c$	2
Zhang et al.'s [25]	$6t_h + 2t_c$	$4t_h + 1t_c + 2t_{sym}$	3
Mishra et al.'s [33]	$2t_c + 8t_h + 1t_{h_b}$	$t_c + 8t_h +$	2
Jiang et al.'s [16]	$2t_h + t_{sym} + t_c$	$2t_h + 2t_{sym} + 3t_c$	2
Hao et al.'s [15]	$2t_c + 3t_h + 2t_{sym}$	$2t_c + 3t_{sym} + 2t_h$	2
Lee's [24]	$2t_c + 7t_h$	$2t_c + 8t_h$	2
Proposed	$3t_c + 1t_{h_b} + 6t_h$	$4t_c + 4t_h$	2

S_9: $U| \equiv \#(Id_{u_i}, T_1, T_2)_{X_U}$
According to the S_8 and S_9, we apply nonce verification rule
S_{10}: $U| \equiv S| \equiv (Id_{u_i}, T_1, T_2)_{X_U}$
With the A3 and S_{10} we concern the jurisdiction rule
S_{11}: $U| \equiv T_2$
According to $Sk_i = h(T_yT_x(Id_i||n_i)||T_zT_y(Id_i||n_i)||T_1)$, S_{11} and A1, we could obtain
S_{12}: $U| \equiv (U \overset{Sk}{\longleftrightarrow} S)$
Hence,we achieved the goal-1 and goal-2 in the proposed scheme which proves security using BAN logic.

Computational Efficiency Analysis

We utilize the following notations t_h, t_{h_b}, T_{me}, T_{fe}, t_b, t_{sym}, t_c, T_{ecm} describing as computation time of hash function, computation time of bio-hashing, computation time of modulo exponentiation, computation time of fuzzy extractor, computation time of bilinear pairing, computation time of symmetric encryption/ decryption, computation time of chaotic map operation, computation time of elliptic curve point multiplication, respectively.

Generally, telecare medicine services rely on devices with limited storage and low computation cost. This makes the necessity of efficient and secure authentication scheme. Although the existing schemes for TMIS guarantee to remove the security weaknesses, still from Tables 1 and 2 it can be seen that these schemes have weak security. In addition, computational overhead of proposed scheme is comparable with related schemes [15, 16, 20, 21, 24] (see Table 4).

Conclusion

In this paper, the security of recently presented chaotic map-based authentication scheme has been illustrated. We have observed the vulnerabilities of existing scheme against stolen smart card attack, identity guessing attack and impersonation attack. Moreover, many schemes provide limited support to unlikability. In order to ensure secure and authorized communication, we developed an authentication protocol relying on the chaotic map for TMIS to achieve desirable security and performance attributes. Note that the proposed protocol overcome the prevalent limitations in existing protocols. In particular, it allows session key verification and mutual authentication with only two messages exchange. Moreover, it ensures forward secrecy along with anonymity and unlinkability. Furthermore, a comparison of proposed construction with existing protocols in terms of computation cost is provided.

Declarations

Research involving human participants and/or animals This article does not contain any studies with human participants or animals performed by any of the authors.

Informed consent All the authors have agreed to this submission.

Disclosure of potential conflicts of interest All authors declare that they have no conflict of interest.

References

1. Wang, Y., Password protected smart card and memory stick authentication against off-line dictionary attacks. IFIP international information security conference. *Springer* 1(1):489–500, 2012.
2. Wazid, M., Das, A. K., Kumar, N., Conti, M., and Vasilakos, A. V., A novel authentication and key agreement scheme for implantable medical devices deployment. *IEEE Journal of Biomedical and Health Informatics, 22*(4), 1299–1309, 2017.
3. Wu, D., and Zhou, C., Fault-tolerant and scalable key management for smart grid. *IEEE Transactions on Smart Grid* 2(2):375–381, 2011.
4. Cao, T., and Zhai, J., Improved dynamic id-based authentication scheme for telecare medical information systems. *Journal of Medical Systems* 37(2):1–7, 2013.

5. Chen, H. M., Lo, J. W., and Yeh, C. K., An efficient and secure dynamic id-based authentication scheme for telecare medical information systems. *Journal of Medical Systems* 36(6):3907–3915, 2012.
6. Gildas, A., Adversarial Model for Radio Frequency Identification. *IACR Cryptology ePrint Archive, 7*, 49–62, 2005.
7. Lin, H. Y., On the security of a dynamic id-based authentication scheme for telecare medical information systems. *Journal of Medical Systems* 37(2):1–5, 2013.
8. Dolev, D., and Andrew, Y., On the security of public key protocols. *IEEE Transactions on Information Theory* 29(2):198–208, 1983.
9. Wei, J., Hu, X., and Liu, W., An improved authentication scheme for telecare medicine information systems. *Journal of Medical Systems* 36(6):3597–3604, 2012.
10. Wu, Z. Y., Lee, Y. C., Lai, F., Lee, H. C., and Chung, Y., A secure authentication scheme for telecare medicine information systems. *Journal of Medical Systems* 36(3):1529–1535, 2012.
11. Xie, Q., Zhang, J., and Dong, N., Robust anonymous authentication scheme for telecare medical information systems. *Journal of Medical Systems* 37(2):1–8, 2013.
12. Zhu, Z., An efficient authentication scheme for telecare medicine information systems. *Journal of Medical Systems* 36(6):3833–3838, 2012.
13. Jiang, Q., Ma, J., Ma, Z., and Li, G., A privacy enhanced authentication scheme for telecare medical information systems. *Journal of Medical Systems* 37(1):1–8, 2013.
14. Guo, C., and Chang, C. C., Chaotic maps-based password-authenticated key agreement using smart cards. *Communications in Nonlinear Science and Numerical Simulation* 18(6):1433–1440, 2013.
15. Hao, X., Wang, J., Yang, Q., Yan, X., and Li, P., A chaotic map-based authentication scheme for telecare medicine information systems. *Journal of Medical Systems* 37(2):1–7, 2013.
16. Jiang, Q., Ma, J., Lu, X., and Tian, Y., Robust chaotic map-based authentication and key agreement scheme with strong anonymity for telecare medicine information systems. *Journal of Medical Systems* 38(2):1–8, 2014.
17. Kohda, T., Tsuneda, A., and Lawrance, A. J., Correlational properties of chebyshev chaotic sequences. *Journal of Time Series Analysis* 21(2):181–191, 2000.
18. Kohda, T., and Tsuneda, A., Pseudonoise sequences by chaotic nonlinear maps and their correlation properties. *IEICE Transactions on Communications* 76(8):855–862, 1993.
19. Niranchana, R., and Karuppiah, M., An efficient and secure remote user mutual authentication scheme using smart cards for Telecare. *Medical Information Systems Informatics in Medicine Unlocked* 16:1–38, 2019.
20. Madhusudhan, R., and Nayak, C. S., A robust authentication scheme for telecare medical information systems. *Multimedia Tools and Applications* 78:15255–15273, 2019.
21. Li, C.-T., Lee, C.-C., Weng, C.-Y., and Chen, S.-j., A secure dynamic identity and chaotic maps based user authentication and key agreement scheme for e-healthcare systems. *Journal of Medical Systems* 40:11–233, 2016.
22. Yu, L., and Kaiping, X., An improved secure and efficient password and chaos-based two-party key agreement protocol. *Nonlinear Dynamics* 84:549–557, 2016.
23. Li, C.-T., Lee, C.-C., and Weng, C.-Y., A secure chaotic maps and smart cards based password authentication and key agreement scheme with user anonymity for telecare medicine information systems. *Journal of Medical Systems* 38:9–86, 2014.
24. Lee, T. F., An efficient chaotic maps-based authentication and key agreement scheme using smartcards for telecare medicine information systems. *Journal of Medical Systems* 37(6):1–9, 2013.
25. Zhang, L., Zhu, S., and Shanyu, T., Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme. *IEEE Journal of Biomedical and Health Informatics* 21(2):465–475, 2017.
26. Burrows, M., Abadi, M., and Needham, R. M., A logic of authentication. Proceedings of the Royal Society of London. *A. Mathematical and Physical Sciences* 426(1871):233–271, 1989.
27. Jiang, Q., Chen, Z., Li, B., Shen, J., Yang, L., and Jianfeng, M., Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems. *Journal of Ambient Intelligence and Humanized Computing* 9:1061–1073, 2018.
28. Wu, F., Xu, L., Kumari, S., Li, X., Das, A. K., and Shen, J., A lightweight and anonymous RFID tag authentication protocol with cloud assistance for e-healthcare applications. *Journal of Ambient Intelligence and Humanized Computing* 9:919–930, 2018.
29. Xu, X., Zhu, P., Wen, Q., Jin, Z., Zhang, H., and He, L., A secure and efficient authentication and key agreement scheme based on ecc for telecare medicine information systems. *Journal of Medical Systems* 38(1):1–7, 2014.
30. Wu, F., and Xu, L., Security analysis and improvement of a privacy authentication scheme for telecare medical information systems. *Journal of Medical Systems* 37(4):1–9, 2013.
31. Lee, T. F., Chang, I. P., Lin, T. H., and Wang, C. C., A Secure and Efficient Password-Based User Authentication Scheme Using Smart Cards for the Integrated EPR Information System. *Journal of Medical Systems* 37(3):1–7, 2013.
32. Jia, X., He, D., Kumar, N., and Choo, K. R., A Provably Secure and Efficient Identity-Based Anonymous Authentication Scheme for Mobile Edge Computing. *IEEE Systems Journal* 14(1):560–571, 2020.
33. Mishra, D., Obaidat, M. S., Rana, S., Dharminder, D., Mishra, A., and Sadoun, B., Chaos-Based Content Distribution Framework for Digital Rights Management System. *IEEE Systems Journal* 15(1):570–576, 2021.
34. Li, C.-T., Shih, D.-H., and Wang, C.-C., Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems. *Computer Methods and Programs in Biomedicine* 157:191–203, 2018.
35. Kumar, V., Ahmad, M., and Kumari, A., A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS. *Telematics and Informatics* 38:100–117, 2019.
36. Salem, F. M., and Amin, R., A privacy-preserving RFID authentication protocol based on El-Gamal cryptosystem for secure TMIS. *Information Sciences* 527:382–393, 2020.
37. Gaikwad, V. P., Tembhurne, J. V., Meshram, C., and Lee, C.-C., Provably secure lightweight client authentication scheme with anonymity for TMIS using chaotic hash function. *The Journal of Supercomputing*, 1–24, 2021.
38. Nayak, P., and Pippal, R. S., Cryptanalysis of Zhian Zhu's Scheme and Evaluation of TMIS Smart Card Authentication Schemes. *Journal of Scientific Research* 13(2):407–413, 2021.