Multimedia Tools and Applications (2019) 78:15255–15273
https://doi.org/10.1007/s11042-018-6884-6

A robust authentication scheme for telecare medical information systems

R. Madhusudhan[1] **· Chaitanya S. Nayak**[1]

Received: 30 January 2018 / Revised: 13 October 2018 / Accepted: 13 November 2018 /
Published online: 29 November 2018

Abstract
With the speedy progress in technology, the Internet has become a non-separable part of human life. It is obvious to use the Internet in all fields and medical field is no exception. The concept of establishing telecare medicine information systems(TMIS) for patients is gaining more popularity recently. To ensure the privacy of patients and to allow authorized access to remote medical servers, many authentication schemes have been proposed. Li et al., in 2016, proposed a secure dynamic identity and chaotic maps based user authentication and key agreement scheme. They claimed that the scheme is resistant to most of the known attacks. However, from thorough cryptanalysis, we have proved that their scheme is vulnerable to user impersonation attack, password guessing attack and server impersonation attack. We have also illustrated that their scheme does not provide user anonymity, convenient smart card revocation and security to session key. To overcome the aforementioned security weaknesses, we have proposed an enhanced authentication scheme using chaotic maps, which has been discussed in this paper along with its cryptanalysis. Cryptanalysis of the proposed scheme proves that the scheme is more robust and suitable for implementation.

Keywords User authentication · Password · Chaotic map · Hash functions · Mutual authentication · Security

1 Introduction

The evolution and swift progress in the Internet technology has left no stone unturned. Digitization is of utmost importance in almost all the fields including e-medicine. Valuable work has been happening lately in this field including applications of IoT, schemes for implantable medical devices deployment and wireless body area networks [3, 4, 37,

✉ R. Madhusudhan
madhu_nitks@yahoo.com

Chaitanya S. Nayak
chaitanyasnayak19@gmail.com

[1] Department of Mathematical and Computational Sciences, National Institute of Technology Karnataka, Surathkal, Karnataka, India

43–45]. Due to this, the geographical distance between patients and doctors is far close to elimination. In medical organizations, medical personnel have to quickly understand the complete information of patients to make instant and accurate diagnoses as well as to provide appropriate treatment.

The purpose of medical records is to provide continuity of care [10]. A patient's medical record is an important part of treatment, and to aid in treatment, the record must contain complete, accurate personal information [38]. Traditional article-based patient records have various drawbacks like disorganization, low data mobility, illegibility, more space requirement, conservation difficulty and low transferability [14, 27, 35, 36, 41, 42]. To overcome all these drawbacks, traditional article-based patient records have been transformed to electronic patient records. The advantages of this approach are accessibility, low costs, easy reporting, readability and diagnostic support [23].

In order to support patients and doctors, the integrated EPR (Electronic Patient Record) systems are widely used. Monitoring patient's health data and providing accurate information to medical institutions, analysis and maintenance of patient's health is mostly covered in EPR information system. Personal health record systems are more than just repositories for patient data; they combine data, knowledge and software tools, which help patients to become active participants in their own care [39]. Doctors use the information (ex. ECG, EEG, treatment record of the diseases, etc.) to diagnose and treat disease [34]. Since the Internet is open to all, it is vulnerable to various security attacks. Patients and physicians fear that medical records may not be secure because the EPR systems are Web-based [2]. A registered user can access services from the medical server whenever required. During these data exchange, a lot of private and sometimes, highly confidential information will be transmitted over public channels. Due to this, there is great risk for loss of privacy and this has to be controlled. For e.g., in the US, federal regulations enacted under the Health Insurance Portability and Accountability Act (HIPAA) require members of the healthcare industry who use electronic information systems to protect the privacy of medical information [5].

To use services from a remote server, one must have proper access rights. Authentication guarantees that the system's resources are not obtained fraudulently by unauthorized users [52]. Password-based authentication scheme is one of the most convenient authentication mechanisms. But due to the openness of the Internet, number of attacks are possible. So, to achieve secure authentication, a strong authentication scheme is essential between user and server.

Different authentication schemes have been proposed in the literature and one such scheme was proposed by Li et al. [22]. The contribution of this article is to reveal the weaknesses of Li et al.'s scheme and propose a robust scheme, which overcomes the mentioned weaknesses.

1.1 Contributions of the paper

Contributions of this paper are as follows:

1. We have proposed an authentication scheme using Chebyshev chaotic maps which provides smaller key size with fast computation and higher efficiency. In this scheme, both the parties can authenticate each other. Also, the proposed scheme does not maintain any user identity or password verification table.
2. Security analysis of the proposed scheme proves that it can overcome all the security attacks. In addition to this, analysis is presented using widely accepted BAN(Burrows-Abadi-Needham) logic. In this, it is proved that the session key generated during a

session is safe. This safety of session key assures that the communication between both the parties is secure. In other words, it can be inferred that the proposed scheme provides security.

3. Comparison of communication cost with real time execution values of the proposed scheme with other schemes have been presented. Additionally, various schemes have been compared based on the performance.

1.2 Structure of the paper

The rest of the article is organized as follows. Section 2 briefly puts light on the related work. Section 3 discusses mathematical preliminaries used in the reviewed and proposed schemes. Section 4 reviews Li et al.'s scheme followed by its cryptyanalysis in Section 5. The proposed scheme is thoroughly explained in Section 6, whereas security analysis of the proposed scheme is discussed in Section 7. Section 8 verifies the proposed scheme using BAN logic. Section 9 compares the proposed scheme with other schemes in terms of computational cost, execution time as well as performance with Section 10 concluding the paper.

2 Related work

In this section, remote user authentication schemes for the integrated EPR information systems have been studied thoroughly. Remote user authentication schemes are employed to ensure secure and authorized communication between user and server [52]. They verify the validity of remote user and server over insecure channel. Several schemes have been proposed in the literature for the integrated EPR information systems to improve the existing schemes. Tsai et al. [40], Madhusudhan and Mittal [25] have clearly explained the possible attacks to consider and the security goals to achieve while designing an ideal authentication scheme using smart cards.

D. Mishra [30], Cao et al. [7] and others have proposed different schemes for the integrated EPR system [9, 31, 32]. In 2010, Wu et al. [52] proposed an efficient user authentication scheme for telecare medicine authentication system with low computational cost. But then, He et al. [12] showed that Wu et al.'s scheme suffered from impersonation attack and insider attack. Then they proposed an improved scheme. In the same year, Wei et al. [46] demonstrated that He et al.'s scheme could not provide two-factor security and proposed an improved scheme. But then, Zhu [55] showed that Wei et al.'s scheme could not resist offline password guessing attack and he proposed RSA-based authentication scheme for TMIS. In these schemes, the identity of the user was static. Later dynamic ID-based authentication schemes for TMIS were proposed. Again in 2012, Wu et al. [51] proposed an efficient password based user authentication scheme using smart cards for the integrated EPR information systems based on difficulty of solving the Discrete Logarithm Problem (DLP). Their scheme consists of lightweight hashing functions and multiplication computations. But in 2013, Lee et al. [21] pointed out that the scheme in [51] was vulnerable to stolen-verifier and smart card loss attacks; they proposed an improved version of that scheme. But then, Wen [47] pointed out that [21] could not withstand offline password guessing attack and he proposed an improvement of the same. Also, in 2013 and 2014, different authentication schemes were proposed [8, 16, 48, 50, 53]. However, Das [11] in 2015, identified the flaws in password change phase of Wen's scheme and also showed that their scheme failed to overcome privileged insider attack. He then proposed an improved version of the Wen's scheme

while retaining the original merits of Lee et al.'s scheme and Wen's scheme, in which it is mentioned that the improved scheme is secure against possible known attacks. Later, Mir et al. [29] pointed out weaknesses in [11] and proposed an improved scheme. Authentication schemes based on chaotic maps were proposed [17, 20, 24, 33].

Recently Li et al. [22] proposed a chaotic map based authentication scheme for e-healthcare systems. In this article, we have thoroughly cryptanalyzed their scheme. Unfortunately, several security weaknesses have been identified, which includes server impersonation attack, failure to provide user anonymity, password guessing attack etc.

3 Mathematical preliminaries

The proposed scheme makes use of one-way hash functions, Chebyshev polynomial and chaotic maps. These maps produce required confusion and diffusion. The outputs produced by chaotic maps combined with hash functions can make it almost impossible for an adversary to guess the values without knowledge of initial values. It is a map which exhibits some sort of random behavior. They are unstable dynamical systems with high sensitivity to initial conditions [13]. In other words, a negligible change in the input makes a huge difference in the resulting output. Properties of chaotic maps like ergodicity and sensitive dependence on initial conditions and system parameters are quite advantageous to construct secure communication schemes, where irregularity in code sequences, sensitive dependence on plain texts and keys are required [26]. In this section, the basics of these concepts are described.

1. Hash function: A one-way cryptographic hash function, $h : \{0,\ 1\}^* \rightarrow \{0,\ 1\}^*$ takes a binary string $q\ \varepsilon\ \{0,\ 1\}^*$ of any arbitrary length as an input and produces a binary string of fixed length, say $n\ bits$, $h(q) \epsilon \{0,\ 1\}^*$ as output [49].
2. Chebyshev polynomial and properties [15, 54]

   – The Chebyshev polynomial $T_n(x) : [-1, 1] \rightarrow [-1, 1]$ of degree n is defined as

$$T_n(x) = \begin{cases} \cos(n.\arccos(x)) & \text{if } x \epsilon [-1, 1] \\ \cos(n\theta) & \text{if } x = \cos\theta, \theta \epsilon [0, \pi] \end{cases} \tag{1}$$

   The recurrence relation of the polynomial in (1) is given by

$$T_n(x) = \begin{cases} 1 & \text{if } n = 0 \\ x & \text{if } n = 1 \\ 2xT_{n-1}(x) - T_{n-2}(x) & \text{if } n \geq 2 \end{cases} \tag{2}$$

   – The semi-group property of the enhanced Chebyshev polynomial holds on the interval $(-\infty, +\infty)$ and is defined as follows
   For $T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x)$, $n \geq 2$ where p is a large prime and $x \epsilon (-\infty, +\infty)$, $T_r(T_s(x)) \equiv T_{rs}(x) \equiv T_s(T_r(x))(mod\ p)$ always holds where $r, s \epsilon Z_p^* = \{a | 0 < a < p,\ gcd(a, p) = 1\} = \{1, 2, ..., p - 1\}$.

   – For any given x and y, it is computationally infeasible to find integer s such that $T_s(x) = y$. This property is referred to as the chaotic map-based discrete logarithm problem (CMDLP).

4 Review of Li et al.'s scheme [22]

In this section, Li et al.'s scheme is briefly reviewed. The notations used in this scheme are listed in Table 1. The various phases of Li et al.'s scheme are given below.

A. **Registration Phase**

To access services from the e-healthcare system server S, a new user U_i must register himself/herself at the server S. The following steps are performed during registration:

R1. U_i initially selects his/her identity ID_i, a password PW_i and a random number b. U_i computes the masked password $W = h(PW_i \parallel b)$ and sends the registration message $\{ID_i, W\}$ to the server S via a secure channel.

R2. On receiving the registration request message $\{ID_i, W\}$ from the user U_i, the server S validates the identity ID_i of U_i. If it is valid, the server S calculates $T_d(ID_i \parallel Q)$ and computes $v = W \oplus T_d(ID_i \parallel Q)$. It then stores ID_i and Q in its database. If it is U_i's initial registration, S sets $Q = 0$ in the field of registration times for U_i; else S sets $Q = Q + 1$.

R3. S then issues a smart card containing the information $\{v, h(.), Q\}$ to the user U_i via a secure channel.

R4. U_i calculates $T_d(ID_i \parallel Q) = v \oplus W$, $X = b \oplus h(ID_i \parallel PW_i)$, $Y = h(T_d(ID_i \parallel Q) \parallel b \parallel h(ID_i \parallel PW_i)$ and stores X and Y into the smart card.

B. **Login Phase**

Whenever a registered user wants to login to the TMIS system server S, the following steps will be executed:

L1. U_i inserts his/her smart card into the card reader of a terminal, inputs his/her identity ID_i and password PW_i. The smart card of U_i computes $h(ID_i \parallel PW_i)$, $b = X \oplus h(ID_i \parallel PW_i)$, $W = h(PW_i \parallel b)$ and $T_d(ID_i \parallel Q) = v \oplus W$. It then verifies if $h(T_d(ID_i \parallel Q) \parallel b \parallel h(ID_i \parallel PW_i)) = Y$ holds or not. If it holds, it goes to next step. Otherwise, the login session is terminated.

L2. U_i's smart card generates a random number a and computes $K_{US} = T_a T_d(ID_i \parallel Q)$, $R = h(ID_i \parallel T_a(ID_i \parallel Q) \parallel T_d(ID_i \parallel Q))$ and $V = K_{US} \oplus (ID_i \parallel R)$.

L3. Finally, U_i sends the login request message $\{T_a(ID_i \parallel Q), V\}$ through a public channel to the server S.

Table 1 Notations used in this article

Symbol	Meaning
U_i	i^{th} user
S/S_j	The integrated EPR information system server
ID_i	Identity of the user U_i
PW_i	Password of the user U_i
d/x	S's private key(Li et al.'s/proposed scheme)
h(.)	Secure collision-free hash function
$T_d(.)$	Chebyshev chaotic map
SK	Established session key between S and U_i
$\parallel$	Concatenation operation
$\oplus$	XOR operation

C. **Authentication Phase**

On receiving the login request message $\{T_a(ID_i \parallel Q), V\}$ from U_i, server S performs the following steps:

A1. S calculates $K_{US}^l = T_d T_a(ID_i \parallel Q)$, verifies the validity of ID_i and Q. It then verifies if $h(ID_i \parallel T_a(ID_i \parallel Q) \parallel T_d(ID_i \parallel Q)) = R$ holds or not. If it does not hold, S rejects the service request message and the authentication phase is terminated.

A2. S computes session key $SK = h(ID_i \parallel T_d(ID_i \parallel Q) \parallel T_a(ID_i \parallel Q))$ and $Z = h(ID_i \parallel SK \parallel T_d(ID_i \parallel Q))$ and sends the authentication request message $\{Z\}$ to the user U_i.

A3. On receiving the authentication request message $\{Z\}$ from S, U_i computes $SK^l = h(ID_i \parallel T_d(ID_i \parallel Q) \parallel T_a(ID_i \parallel Q))$ to check if the condition $h(ID_i \parallel SK^l \parallel T_d(ID_i \parallel Q)) = Z$ holds or not. If the condition holds, the server S is authenticated.

After successful authentication, the session key $SK = h(ID_i \parallel T_d(ID_i \parallel Q) \parallel T_a(ID_i \parallel Q)) = SK^l$ provides a secure channel for S and U_i to communicate with each other.

D. **Password Change Phase**

Suppose a user U_i wants to change the password, the following steps are performed:

P1. U_i inserts his/her smart card into the card reader terminal, enters his/her identity ID_i and old password PW_i. The smart card computes $h(ID_i \parallel PW_i)$, $b = X \oplus h(ID_i \parallel PW_i)$, $W = h(PW_i \parallel b)$, $T_d(ID_i \parallel Q) = v \oplus W$ and verifies if $h(T_d(ID_i \parallel Q) \parallel b \parallel h(ID_i \parallel PW_i))$ equals Y or not. If the verification is valid, U_i enters a new password PW_{new}; else the request is denied.

P2. The smart card computes $W_{new} = h(PW_{new} \parallel b)$, $v_{new} = W_{new} \oplus T_d(ID_i \parallel Q)$, $X_{new} = b \oplus h(ID_i \parallel PW_{new})$ and $Y_{new} = h(T_d(ID_i \parallel Q) \parallel b \parallel h(ID_i \parallel PW_{new}))$.

P3. Finally, the smart card replaces v, X and Y with v_{new}, X_{new} and Y_{new} respectively.

E. **Smart Card Revocation Phase**

Suppose a legal user U_i loses his/her smart card, U_i informs S regarding his/her revocation in person. S then confirms the authenticity of U_i by verifying U_i's identification papers. On successful authentication, S asks U_i to select a new password and a new random number and execute the same steps of the registration phase. Finally S sets $Q = Q + 1$ in the field of registration times for U_i.

5 Security weaknesses in Li et al.'s scheme

In this section, Li et al.'s scheme has been cryptanalyzed in depth and identified weaknesses are explained in detail. Before analyzing the scheme, the following assumptions are considered regarding the possibilities of an adversary as described by Kocher et al. [19] and Messerges et al. [28]:

1. An adversary has total control over the communication channel connecting the users and the remote server in login/authentication phase. So the adversary can intercept, insert, delete or modify any message transmitted via public channel.

2. An adversary can extract the information stored in a smart card by means of analyzing the power consumption of the smart card.

5.1 Obtaining secret value d of the server *S*

Suppose an adversary initially registers as a legal user in the system with his own ID and PW, then the system issues a smart card with all registered parameters in it. Now, according to Kocher et al. and Messerges et al., the adversary can obtain all the parameters inside the card. So the adversary now has the parameters $\{X,\ Y,\ h(.),\ v,\ Q\}$ stored in it by analyzing the power consumption. Now, he calculates $T_d(ID \parallel Q) = v \oplus W$, where $W = h(PW_i \parallel b)$, password and random number are of the adversary. He then calculates

$$d^l = \frac{\arccos T_d(ID_i||Q) + 2k\pi}{\arccos(x)}$$

such that $T_d^l(ID \parallel Q) = T_d(ID \parallel Q)$.

1. **No user anonymity**
   Assume that the adversary comes in possession of the smart card of a user U_i with the values $\{X,\ Y,\ h(.),\ v,\ Q\}$ and he has stored these values. Suppose he eavesdrops the login message $\{T_a(ID_i \parallel Q),\ v\}$ and authentication message $\{Z\}$ between U_i and S, then from the above argument, adversary calculates $a^l = \frac{\arccos T_a(ID_i||Q)+2k\pi}{\arccos(x)}$ such that $T_a^l(ID_i \parallel Q) = T_a(ID_i \parallel Q)$. He then chooses ID^l, computes $T_a^l(ID^l \parallel Q)$ using the value of Q stored in the smart card and checks if the computed value equals $T_a(ID_i \parallel Q)$. If they are equal, the adversary has guessed the correct identity. If not, he repeats the procedure with different values for ID until he guesses the correct identity. So, user anonymity is not preserved in this scheme.

2. **Vulnerable to password guessing attack**
   Suppose an adversary gets a smart card having the values $\{X,\ Y,\ h(.),\ v,\ Q\}$, which he stores for his further purposes, and has eavesdropped login message $\{T_a(ID_i \parallel Q),\ v\}$ and authentication message $\{Z\}$ between U_i and S. From 1), the adversary already has obtained the ID_i of U_i. Also he has originally calculated d^l such that $T_d^l(ID \parallel Q) = T_d(ID \parallel Q)$. Now using ID_i and Q from smart card, he computes $T_d^l(ID_i \parallel Q)$ which is $T_d(ID_i \parallel Q)$. Using $v = W \oplus T_d(ID_i \parallel Q)$, adversary computes $W = v \oplus T_d(ID_i \parallel Q)$. Also from $X = b \oplus h(ID_i \parallel PW_i)$, b is computed as $b = X \oplus h(ID_i \parallel PW_i)$. The value $Y = h(T_d(ID_i \parallel Q) \parallel b \parallel h(ID_i \parallel PW_i))$ is stored in the smart card. Substituting b in this expression, $Y = h(T_d^l(ID_i \parallel Q) \parallel X \oplus h(ID_i \parallel PW_i) \parallel h(ID_i \parallel PW_i))$ where X is obtained from the smart card. Now adversary guesses a value PW, computes $Y^l = h(T_d^l(ID_i \parallel Q) \parallel X \oplus h(ID_i \parallel PW) \parallel h(ID_i \parallel PW))$ and checks if $Y^l = Y$ holds. If it holds, adversary has guessed the correct password. If not, he repeats the procedure with different values for PW until he guesses the correct value. So the scheme cannot provide protection against offline password guessing attack.
3. **Vulnerable to user impersonation attack**
   Assume that an adversary has the values ID_i and PW_i of a legal user along with the stored smart card values $\{X,\ Y,\ h(.),\ v,\ Q\}$. He chooses a random number a^{ll} and computes $T_a^{ll}(ID_i \parallel Q)$ from the stored value Q. He further computes $K_{US}^{ll} = T_a^{ll} T_d^l(ID_i||Q)$, $R^{ll} = h(ID_i \parallel T_a^{ll}(ID_i \parallel Q) \parallel T_d^l(ID_i \parallel Q))$ and $v_1^l = K_{US}^{ll} \oplus (ID_i \parallel R^{ll})$, sends the login request message $\{T_a^{ll}(ID_i \parallel Q),\ v^{ll}\}$ to the server S.

On receiving this message, server does the required computations including the session key, $SK^{ll} = h(ID_i \parallel T_d^l(ID_i \parallel Q) \parallel T_a^{ll}(ID_i \parallel Q))$ and sends Z^{ll} to the user, where $Z^{ll} = h(ID_i \parallel SK^{ll} \parallel T_d^l(ID_i \parallel Q))$. So, the adversary successfully impersonated as the legal user. Hence, their scheme cannot resist user impersonation attack.

4. **Inconvenient smart card revocation phase**

   In this scheme, if a legal user wants to revoke a lost smart card, he/she must inform the medical server in person meaning revocation cannot take place online and the user has to be physically present causing inconvenience to the user and hence it can be concluded that smart card revocation is not very convenient from the point of view of the user.

5. **Insecure session key**

   Assume that an adversary has eavesdropped the login message $\{T_a(ID_i \parallel Q),\ v\}$ as well as the authentication message $\{Z\}$ of a user and has stored the values from the smart card. As explained in 1), adversary can obtain the ID_i. Also he has the value of $T_a(ID_i \parallel Q)$ from the login message and he has calculated d^l such that $T_d^l(ID_i \parallel Q) = T_d(ID_i \parallel Q)$. He can easily compute the session key as $SK = h(ID_i \parallel T_d^l(ID_i \parallel Q)||T_a(ID_i \parallel Q))$. Therefore, the session key is not secure in their scheme.

6. **Vulnerable to server impersonation attack**

   As explained in 1), an adversary has user identity ID_i from the smart card and obtains the required password PW_i of the user U_i as explained in 2). Also, he has the value $T_d^l(ID_i \parallel Q) = T_d(ID_i \parallel Q)$ as explained above. Assume that the adversary obtains the user login request message $\{T_a(ID_i \parallel Q),\ v\}$. Using $T_d^l(ID_i \parallel Q)$, he computes $SK = h(ID_i \parallel T_d^l(ID_i \parallel Q) \parallel T_a(ID_i \parallel Q))$, $Z = h(ID_i \parallel SK \parallel T_d(ID_i \parallel Q))$ and sends the $\{Z\}$ to the user U_i. On receiving $\{Z\}$, U_i computes $SK_l = h(ID_i \parallel T_d(ID_i \parallel Q) \parallel T_a(ID_i \parallel Q))$ and the condition $h(ID_i \parallel SK^l \parallel T_d(ID_i \parallel Q)) = Z$ holds since $T_d^l(ID_i \parallel Q) = T_d(ID_i \parallel Q)$. User authenticates him as the authentic server and communicates with him proving that the adversary has successfully impersonated the server.

7. **Vulnerable to man-in-the-middle attack**

   As explained in 3) and 6), an adversary can impersonate a legal user, U_i and can masquerade a server S_i. This can be a done in the session wherein an adversary impersonates the legal user, U_i and server S. In other words, he can easily perform man-in-the-middle attack and their scheme cannot resist this attack.

6 The proposed scheme

In this section, the proposed scheme is explained in detail. Assuring secure communication between user and server being the primary concern, chaotic maps have been used in the proposed scheme.

A. **Registration Phase**

To access services from a trusted medical server, new user U_i has to register himself/herself initially. This phase is shown in Fig. 1. The steps in this phase are as follows.

R1. User U_i chooses a username ID_i, a password PW_i and a secret number b. Then he computes the masked password $A_i = b \oplus h(ID_i \parallel PW_i)$ and sends the registration message $\{ID_i,\ A_i\}$ to the server S_j via a secure channel.

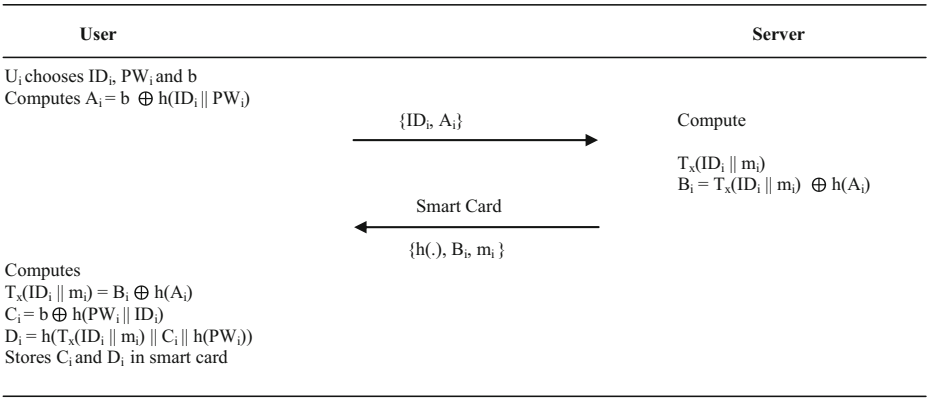

Fig. 1 Registration phase of the proposed scheme

R2. On receiving the registration request message $\{ID_i,\ A_i\}$ from the user U_i, the server S_j validates the identity ID_i of U_i. If it is valid, the server S_j computes $T_x(ID_i \parallel m_i)$, where x is the secret key of the server and m_i is a random number chosen by server for U_i(which is unique for every user). It then computes $B_i = T_x(ID_i \parallel m_i) \oplus h(A_i)$.

R3. S_j then issues a smart card containing the information $\{h(.),\ B_i,\ m_i\}$ to the user U_i via a secure channel.

R4. After receiving the smart card securely from the server S_j, U_i computes $T_x(ID_i \parallel m_i) = B_i \oplus h(A_i)$, $C_i = b \oplus h(PW_i \parallel ID_i)$, $D_i = h(T_x(ID_i||m_i)||C_i||h(PW_i))$ and stores C_i and D_i in the smart card.
This completes the registration phase of a new user U_i and Fig. 1 represents this phase. The smart card now has the values $\{B_i,\ h(.),\ C_i,\ D_i,\ m_i\}$ stored in it.

B. **Login Phase**

If a registered user wants to login to the TMIS server S_j, the following steps will be executed:

L1. U_i inserts his/her smart card into the card reader of a terminal, inputs his/her identity ID_i and password PW_i. The smart card of U_i computes $b^l = C_i \oplus h(PW_i \parallel ID_i)$ and $A_i^l = b^l \oplus h(ID_i \parallel PW_i)$.

L2. Using A_i^l, the smart card obtains $T_x(ID_i \parallel m_i)^l = h(A_i^l) \oplus B_i$ and computes $D_i^l = h(T_x(ID_i||m_i)^l||C_i||h(PW_i))$. Then it checks if $D_i^l = D_i$ holds or not. If it does not hold, the session is aborted. Else step L3 is executed.

L3. The smart card computes generates a random number y and computes $E_i = h(D_i) \oplus T_y(ID_i \parallel m_i)$, $CID_i = h(ID_i) \oplus T_y(T_x(ID_i \parallel m_i))$ and $F_i = h(E_i \parallel T_y(ID_i \parallel m_i) \parallel h(ID_i))$. Finally the smart card of U_i sends the login request message $\{CID_i,\ D_i,\ E_i,\ F_i\}$ to S_j through a public channel.

C. **Authentication Phase**

On receiving the login request message $\{CID_i,\ D_i,\ E_i,\ F_i\}$ from U_i, server S_j performs the following steps to authenticate the user U_i:

A1. S_j obtains $T_y(ID_i \parallel m_i) = h(D_i) \oplus E_i$ and computes $h(ID_i) = CID_i \oplus T_x(T_y(ID_i \parallel m_i))$. Then it computes $h(E_i \parallel T_y(ID_i \parallel m_i) \parallel h(ID_i))$ and checks

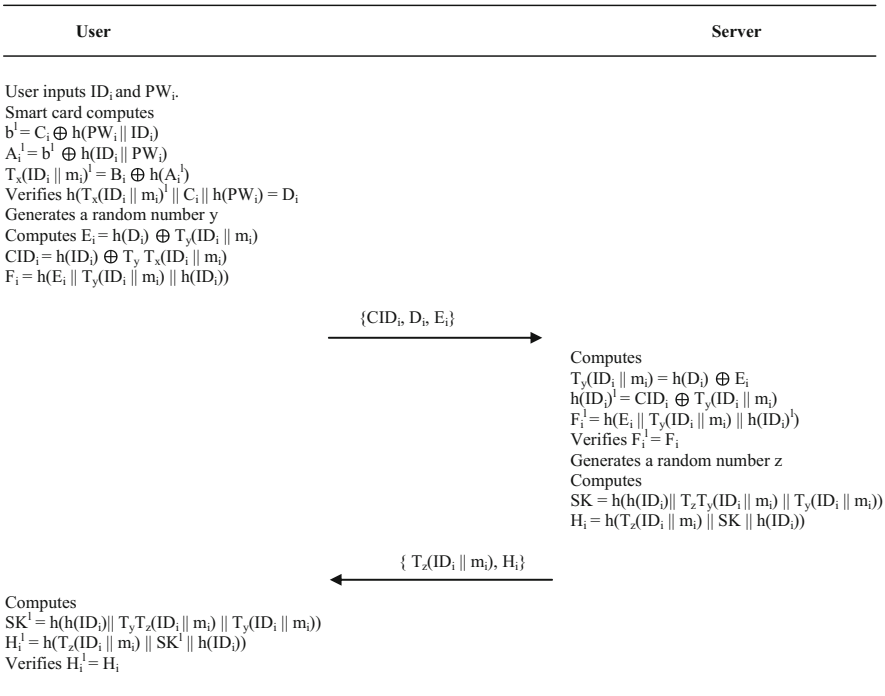

Fig. 2 Login and authentication phases of the proposed scheme

if it is equal to F_i received in the login message. If equal, S_j authenticates U_i and executes step A2; otherwise this session is terminated.

A2. S_j generates a random number z and computes the session key, $SK = h(h(ID_i)||T_z(T_y(ID_i||m_i))||T_y(ID_i||m_i))$ and $H_i = h(T_z(ID_i \| m_i) \| SK \| h(ID_i))$. Then it sends the authentication message $\{T_z(ID_i \| m_i), H_i\}$ to U_i through a public channel.

A3. On receiving $\{T_z(ID_i \| m_i), H_i\}$ from S_j, U_i computes $SK^l = h(h(ID_i)||T_z(T_y(ID_i||m_i))||T_y(ID_i||m_i))$ and $H_i^l = h(T_z(ID_i||m_i)) \| SK^l \| h(ID_i))$. Then it verifies if the condition $H_i^l = H_i$ holds or not. If it holds, U_i authenticates S_j. Else, U_i aborts the session.
After mutual authentication, U_i and S_j agree on the shared session key, $SK = h(h(ID_i)||T_z(T_y(ID_i||m_i))||T_y(ID_i||m_i))$ to communicate with each other and this completes the authentication phase.

Figure 2 demonstrates the login as well as authentication phases of the proposed scheme.

D. **Password Change Phase**

Suppose a user wants to change or update his/her password, the following steps will be performed:

P1. U_i inserts his/her smart card into the card reader of a terminal, inputs his/her identity ID_i and password PW_i. The smart card of U_i computes $b^l = C_i \oplus h(PW_i \|$

ID_i) and $A_i^l = b^l \oplus h(ID_i \parallel PW_i)$. Using A_i^l, the smart card obtains $T_x(ID_i \parallel m_i)^l = h(A_i^l) \oplus B_i$ and computes $D_i^l = h(T_x(ID_i||m_i)^l||C_i||h(PW_i))$. Then it checks if $D_i^l = D_i$ holds or not. If it does not hold, the session is aborted and user cannot change password. Else, the server requests for a new password from the user.

P2. User U_i enters the new password PW_i^{new}. The smart card computes $A_i^{new} = b \oplus h(ID_i \parallel PW_i^{new})$, $B_i^{new} = h(A_i^{new}) \oplus T_x(ID_i \parallel m_i)$, $C_i^{new} = b \oplus h(PW_i^{new} \parallel ID_i)$ and $D_i^{new} = h(T_x(ID_i||m_i)^l||C_i^{new}||h(PW_i^{new}))$. It then replaces the values B_i, C_i and D_i with B_i^{new}, C_i^{new} and D_i^{new} respectively.

This completes the password change phase.

E. **Smart Card Revocation Phase**

If a user loses his/her smart card, he/she can send an online request to the server entering the identity ID_i. After checking if that ID_i is valid, the user has to answer the security questions. On successful verification of the legality of the user, the server deactivates the old smart card concerned with that ID_i and requests the user to enter a new masked password A_i^{new}. Using A_i^{new} and ID_i, the server does the required computations as in registration phase and issues a new smart card to the user with the newly computed values. On receiving the new smart card, the user computes C_i and D_i and stores them in the smart card.

7 Security analysis

Security analysis of the proposed scheme has been discussed in this section. It is shown that the proposed scheme overcomes all the security weaknesses pointed out in Li et al.'s scheme.

1. **User anonymity is preserved**

The identity ID_i of user is not stored in smart card and in login phase, identity is sent as dynamic identity CID_i, which changes during every session. Suppose an adversary eavesdrops the login and/or authentication messages, $\{CID_i,\ D_i,\ E_i,\ F_i\}$ and/or $\{T_z(ID_i \parallel m_i),\ H_i\}$ respectively of the user U_i, revealing ID_i is impossible due to CMDLP explained in 2) of Section 3. It is computationally infeasible to obtain value of ID_i without knowledge of x and y in $T_yT_x(ID_i \parallel m_i)$. Hence, the user anonymity is preserved in the proposed scheme.

2. **Security against password guessing attack**

In the proposed scheme, the password PW_i of a user U_i is covered with his/her own secret value b and identity ID_i. Now suppose an adversary gets to know ID_i, it is not possible to guess PW_i without the knowledge of b, which is a secret number known only to the user U_i. Suppose the adversary obtains the values $\{A_i,\ h(.),\ B_i,\ C_i,\ D_i\}$ from the smart card of the user U_i, even then the scheme forbids password guessing because the password PW_i is protected with secret key, x of the server as well as ID_i and b in $D_i = h(T_x(ID_i||m_i)||C_i||h(PW_i))$ and $A_i = b \oplus h(ID_i \parallel PW_i)$. Therefore, the proposed scheme resists offline password guessing attack.

3. **Security against user impersonation attack**

Since random numbers are generated during every session, impersonation attack is not possible. If an adversary has all the smart card values $\{h(.),\ C_i,\ D_i,\ B_i,\ m_i\}$ and previously intercepted login message $\{CID_i,\ D_i,\ E_i,\ F_i\}$, it is not possible to

generate a valid login message in the next session since a nonce, y have been used in the proposed scheme. Guessing these values and forming a valid login message is practically impossible. So, protection against impersonation attack is provided in the proposed scheme.

4. **Efficient smart card revocation**
   Unlike Li et al.'s scheme, the user need not go in person to revoke a lost smart card. He/she has to send an online request and verify his/her identity after which a new smart card will be issued. It has to be noted that in the proposed scheme, server deactivates the old smart card on verification of the legality of the user of the lost smart card so that even if adversary comes in possession with that card, he/she cannot misuse the card. So, smart card revocation is efficient in the proposed scheme.
5. **Secure session key**
   In the proposed scheme, the session key SK computed in steps A2 and A3 contains two random numbers y and z combined with Chebyshev chaotic map. If the adversary gets to know these numbers during any session, even then session key cannot be compromised because these random numbers vary during each session with which the session key keeps changing. Along with the knowledge of y and y, an adversary needs to have the correct ID_i to obtain the session key of the user U_i. Also if the adversary gets to know a previous session key, still it will not help him in computing the next session key due to its format, $SK = h(h(ID_i)||T_z(T_y(ID_i||m_i))||T_y(ID_i||m_i))$. So, the session key is well protected in the proposed scheme.
6. **Security against server impersonation attack**
   Random numbers are generated to compute the chaotic values used in the proposed scheme because of which server impersonation is not possible. If an adversary has all the smart card values $\{h(.),\ C_i,\ D_i,\ B_i,\ m_i\}$ and previously intercepted login message $\{CID_i,\ D_i,\ E_i,\ F_i\}$, it is not possible to generate a valid authentication message in the next session since a nonce, z have been used in the proposed scheme. Guessing these values and forming a valid authentication message is impossible. So, protection against server impersonation attack is provided in the proposed scheme.
7. **Resists man-in-the-middle attack**
   It is explained in 3) that the proposed scheme overcomes user impersonation attack. Also, it can withstand server impersonation attack which is justified in 6). In other words, it is not possible for an adversary to impersonate a legal user as well as the server in the same session. This proves that the proposed scheme resists man-in-the-middle attack.

8 Security analysis using ban logic

BAN logic [6] is an analysis model for authentication models. It is used to verify whether the protocol proves the presence of each party to the other and also helps bring to light the various security problems. For verification, the following notations and constructs are used:

1. P believes X ($P \mid\equiv X$) : Principal P acts as though X is true.
2. P sees X ($P \triangleleft X$) : Someone has sent a message containing X to P, who can read and repeat X.
3. P said X ($P \mid\sim X$) : Principal P at some time sent a message including the statement X.

4. P controls X ($P \mid\Rightarrow X$) : P has jurisdiction over X meaning P is an authority on X and should be trusted on this matter.
5. fresh(X) (#(X)) : Formula X is fresh meaning that X has not been sent in a message at any time before the current run of the protocol. This is usually true for nonces.
6. $P \overset{K}{\leftrightarrow} Q$: P and Q may use the shared key K to communicate. The key K will never be discovered by any principal except P or Q, or a principal trusted by either P or Q.
7. $\mid\overset{K}{\rightarrow} P$: P has K as a public key. The matching secret key K^{-1} will never be discovered by any principal except P or a principal trusted by P.
8. $P \overset{X}{=\!=} Q$: Formula X is a secret known only to P and Q, and possibly to principals trusted by them. Only P and Q may use X to prove their identities.
9. $\{X\}_K$: Formula X is encrypted under the key K.
10. $\langle X\rangle_Y$: Formula X is combined with the formula Y, it is intended that Y be a secret and that its presence proves the identity of whoever utters $\langle X\rangle_Y$.

The protocol analysis along with the above constructs uses the following logical postulates in proving the identity of the parties involved.

1. The *message-meaning* rule concerns the interpretation of messages. They all explain how to derive beliefs about the origin of messages.
   For shared keys,
   $$\frac{P \text{ believes } P \overset{K}{\leftrightarrow} Q,\ P \text{ sees } \{X\}_K}{P \text{ believes } Q \text{ said } X}$$
   For public keys,
   $$\frac{P \text{ believes } P \overset{K}{\leftrightarrow} Q,\ P \text{ sees } \{X\}_{K^{-1}}}{P \text{ believes } Q \text{ said } X}$$
   For shared secrets,
   $$\frac{P \text{ believes } P \overset{X}{=\!=} Q,\ P \text{ sees } \langle X\rangle_Y}{P \text{ believes } Q \text{ said } X}$$
2. The nonce-verification rule expresses the check that a message is recent and hence, the sender still believes in it.
   $$\frac{P \text{ believes } \#(X),\ P \text{ believes } Q \text{ said } X}{P \text{ believes } Q \text{ believes } X}$$
3. The jurisdiction rule states that if P believes that Q has jurisdiction over X, then P trusts Q on the truth of X.
   $$\frac{P \text{ believes } Q \text{ controls } X,\ P \text{ believes } Q \text{ believes } X}{P \text{ believes } X}$$
4. If a principal sees a formula, then he also sees its components, provided he knows the necessary keys.
   $$\frac{P \text{ sees } (X, Y)}{P \text{ sees } X}$$
   $$\frac{P \text{ believes } \langle X\rangle_Y}{P \text{ sees } X}$$
   $$\frac{P \text{ believes } P \overset{K}{\leftrightarrow} Q,\ P \text{ sees } \langle X\rangle_K}{P \text{ sees } X}$$
   $$\frac{P \text{ believes } \mid\overset{K}{\rightarrow} P,\ P \text{ sees } \langle X\rangle_K}{P \text{ believes sees } X}$$

$$\frac{P \ believes \ |\xrightarrow{K} P, \ P \ sees \ \langle X \rangle_{K^{-1}}}{P \ believes \ sees \ X}$$

5. The freshness rule indicates that if one part of formula is fresh, then the entire formula is fresh.

$$\frac{P \ believes \ \#(X)}{P \ believes \ \#(X, Y)}$$

Idealized protocol:

Here, $s_2 = T_x(ID_i \parallel m_i)$

$U \rightarrow S : \langle ID \rangle_{U \overset{s_2}{\leftrightarrow} S}, \langle ID \rangle_{\{U \overset{s_2}{\leftrightarrow} S\}_y}, (U \overset{SK}{\leftrightarrow} S, \{U \overset{s_2}{\leftrightarrow} S\}_{r_2})_{U \overset{s_2}{\leftrightarrow} S}$

$S \rightarrow U : (U \overset{SK}{\leftrightarrow} S, \{U \overset{s_2}{\leftrightarrow} S\}_y)_{U \underset{\leftrightarrow}{s_2} S}, \langle ID \rangle_{\{U \overset{s_2}{\leftrightarrow} S\}_z}$

According to the logical postulates, the proposed scheme should satisfy the following goals:

G1. $U \mid\equiv S \mid\equiv U \overset{SK}{\leftrightarrow} S$

G2. $S \mid\equiv U \mid\equiv U \overset{SK}{\leftrightarrow} S$

The following assumptions are made to achieve the desired goals:

A1. $S \mid\equiv U \mid\Rightarrow U \overset{SK}{\leftrightarrow} S$

A2. $U \mid\equiv S \mid\Rightarrow U \overset{SK}{\leftrightarrow} S$

A3. $U \mid\equiv \#(y)$

A4. $S \mid\equiv \#(z)$

A5. $U \mid\equiv U \overset{s_2}{\leftrightarrow} S$

A6. $S \mid\equiv U \overset{s_2}{\leftrightarrow} S$

Analysis:

P1. Since $U \triangleleft (U \overset{SK}{\leftrightarrow} S, \{U \overset{s_2}{\leftrightarrow} S\}_y)_{U \underset{\leftrightarrow}{s_2} S}$, applying message-meaning rule using A5, we obtain $(U \overset{SK}{\leftrightarrow} S, \{U \overset{s_2}{\leftrightarrow} S\}_y)$.

P2. From A3 and P1, application of nonce-verification rule yields $(U \overset{SK}{\leftrightarrow} S, \{U \overset{s_2}{\leftrightarrow} S\}_y)$.

P3. From P2 and A5, we can break the conjunction to obtain $U \mid\equiv S \mid\equiv U \overset{SK}{\leftrightarrow} S$ (G1 is achieved).

P4. Since $S \triangleleft (U \overset{SK}{\leftrightarrow} S, \{U \overset{s_2}{\leftrightarrow} S\}_z)_{U \overset{s_2}{\leftrightarrow} S}$, using A6 and applying message-meaning rule, we obtain $S \mid\equiv U \mid\sim (U \overset{SK}{\leftrightarrow} S, \{U \overset{s_2}{\leftrightarrow} S\}_z)$.

P5. From A4 and P4, using nonce-verification rule, we obtain $S \mid\equiv U \mid\equiv (U \overset{SK}{\leftrightarrow} S, \{U \overset{s_2}{\leftrightarrow} S\}_z)$.

P6. Using P5 and A6, we obtain $S \mid\equiv U \mid\equiv U \overset{SK}{\leftrightarrow} S$ (G2 is achieved).

From G1 and G2, it can be observed that both the user U_i and server S_j believe that the session key $SK = h(T_z(T_y(ID_i \parallel m_i)) \parallel h(ID_i \parallel T_y(ID_i \parallel m_i))$ is shared between them.

Table 2 Computational cost comparison

Phase	Li et al. [22]	Das [11]	Mir et al. [29]	Amin and Biswas [1]	Proposed scheme
Registration	$3T_h + 1T_{ch}$	$4T_h$	$5T_h$	$5T_h$	$5T_h + 1T_{ch}$
Login	$4T_h + 2T_{ch}$	$4T_h$	$6T_h$	$6T_h + 1T_e$	$7T_h + 2T_{ch}$
Authentication	$5T_h + 2T_{ch}$	$11T_h$	$11T_h$	$9T_h + 1T_e$	$6T_h + 2T_{ch}$
Total	$12T_h + 5T_{ch}$	$19T_h$	$22T_h$	$20T_h + 2T_e$	$18T_h + 5T_{ch}$

9 Performance and computational cost comparison

In this section, a detailed comparison of the proposed scheme with Li et al.'s scheme and other schemes [1, 11, 22, 29] has been made in terms of computational cost, execution time and performance. Table 2 shows the computational cost comparison in which, T_h denotes the time required for executing one-way hash operation, T_e for executing exponentiation and T_{ch} for executing $T_n(x)(mod\ p)$ in Chebyshev chaotic map. Concatenation and XOR operations are ignored since their execution time is very less compared to hash functions and chaotic maps. Table 3 compares the execution time of different schemes whereas comparison of performance of the proposed scheme with other schemes is presented in Table 4.

From Table 2, it can be observed that the proposed scheme requires five hash operations more than that of Li et al.'s scheme but the number of chaotic operations is same. But when compared to [11], the proposed scheme uses one hash operation less. From Table 4, it can be clearly seen that even with less hash operations, the proposed scheme is able to provide more security than [11]. In comparison with [1] also, the proposed scheme uses less hash functions. Furthermore, it has to be noted that [1] uses RSA algorithm which increases the time complexity whereas the proposed scheme does not use RSA algorithm and only use of hash operations and chaotic maps.

Table 3 presents the execution time for the aforementioned authentication schemes. The results in this table are computed based on an experiment conducted on Intel Pentium4 2600MHz processor with 1024 MB RAM in [18]. According to this study, the execution time for various operations are $T_h = 0.0005s$, $T_e = 0.063075s$ and $T_{ch} = 0.02102s$. From Table 3, it is clear that the proposed scheme requires 0.002s more than [22]. But this extra time can be justified from Table 4 by noting that the proposed scheme is able to overcome seven security attacks thereby providing more security than [22]. The scheme in [29] requires 0.011s for execution but at the same time, the scheme is not user friendly since there is no option for smart card revocation. The execution time for the scheme in [1] is 0.13615s which is more than the execution time of the proposed scheme. In addition to this, their scheme does not withstand all the security attacks. Also from Table 4, it is clear that

Table 3 Execution time comparison

Phase	Li et al. [22]	Das [11]	Mir et al. [29]	Amin and Biswas [1]	Proposed scheme
Registration	0.02252	0.002	0.0025	0.0025	0.02352
Login	0.04404	0.002	0.003	0.066075	0.04454
Authentication	0.04454	0.0055	0.0055	0.067575	0.04504
Total	0.1111	0.0095	0.011	0.13615	0.1131

Table 4 Performance comparison

Security properties	Li et al. [22]	Das [11]	Mir et al. [29]	Amin and Biswas [1]	Proposed scheme
Provides user anonymity	No	No	Yes	Yes	Yes
Resists user impersonation	No	No	Yes	No	Yes
Resists stolen-verifier attack	Yes	Yes	Yes	Yes	Yes
Resists replay attack	Yes	Yes	Yes	No	Yes
Secure session key	No	No	Yes	Yes	Yes
Mutual authentication	Yes	Yes	Yes	Yes	Yes
Resists offline password guessing	No	No	Yes	No	Yes
Resists man-in-the-middle attack	No	No	Yes	Yes	Yes
Resists server impersonation	No	No	Yes	Yes	Yes
Resists privileged insider attack	Yes	Yes	Yes	Yes	Yes
Resists parallel session attack	Yes	Yes	Yes	Yes	Yes
Efficient smart card revocation	No	No	No	No	Yes

[1] cannot resist user impersonation, replay attack etc. From this, the schemes using less hash operations are not able to overcome all the attacks but the proposed scheme overcomes all the possible security attacks. To achieve these properties, it is worth the additional operations. So, the proposed scheme is robust and more secure when compared to Li et al.'s and the other schemes.

10 Conclusion

Li et al. proposed a secure dynamic identity and chaotic maps based user authentication and key agreement scheme for ehealthcare systems in 2016. Their scheme has been thoroughly cryptanalyzed and several security weaknesses have been pointed out. This paper clearly explains the identified weaknesses which are user impersonation attack, password guessing attack, server impersonation attack, no user anonymity, insecure session key, man-in-the-middle attack and inconvenient smart card revocation. To overcome the mentioned weaknesses, a robust scheme has been proposed using Chebyshev polynomial. The proposed scheme overcomes all the mentioned security weaknesses and is more suitable in terms of security as well as practical implementation.

References

1. Amin R, Biswas G (2015) An improved rsa based user authentication and session key agreement protocol usable in tmis. J Med Syst 39(8):79
2. Anderson JG (2007) Social, ethical and legal barriers to e-health. Int J Med Inf 76(5):480–483
3. Bai T, Lin J, Li G, Wang H, Ran P, Li Z, Li D, Pang Y, Wu W, Jeon G (2018) A lightweight method of data encryption in bans using electrocardiogram signal, Future Generation Computer Systems

4. Bhatt C, Dey N, Ashour AS (2017) Internet of things and big data technologies for next generation healthcare
5. Breaux T, Antón A (2008) Analyzing regulatory rules for privacy and security requirements. IEEE Trans Softw Eng 34(1):5–20
6. Burrows M, Abadi M, Needham RM (1989) A logic of authentication. In: Proceedings of the royal society of London a: mathematical, physical and engineering sciences, vol 426, pp 233–271 The Royal Society
7. Cao T, Zhai J (2013) Improved dynamic id-based authentication scheme for telecare medical information systems. J Med Syst 37(2):9912
8. Chaturvedi A, Mishra D, Mukhopadhyay S (2013) Improved biometric-based three-factor remote user authentication scheme with key agreement using smart card. In: International conference on information systems security, pp 63–77 Springer
9. Chen HM, Lo JW, Yeh CK (2012) An efficient and secure dynamic id-based authentication scheme for telecare medical information systems. J Med Syst 36(6):3907–3915
10. Chen TL, Chung YF, Lin FY (2012) A study on agent-based secure scheme for electronic medical record system. J Med Syst 36(3):1345–1357
11. Das AK (2015) A secure and robust password-based remote user authentication scheme using smart cards for the integrated epr information system. J Med Syst 39(3):25
12. Debiao H, Jianhua C, Rui Z (2012) A more secure authentication scheme for telecare medicine information systems. J Med Syst 36(3):1989–1995
13. Devaney RL, Siegel PB, Mallinckrodt AJ, McKay S (1993) A first course in chaotic dynamical systems: theory and experiment. Comput Phys 7(4):416–417
14. Hannan TJ (1996) Electronic medical records. Health Inf an Overview, vol 133
15. He D, Bu J, Chan S, Chen C, Yin M (2011) Privacy-preserving universal authentication protocol for wireless communications. IEEE Trans Wirel Commun 10(2):431–436
16. Jiang Q, Ma J, Ma Z, Li G (2013) A privacy enhanced authentication scheme for telecare medical information systems. J Med Syst 37(1):9897
17. Jiang Q, Wei F, Fu S, Ma J, Li G, Alelaiwi A (2016) Robust extended chaotic maps-based three-factor authentication scheme preserving biometric template privacy. Nonlinear Dynamics 83(4):2085–2101
18. Kocarev L, Lian S (2011) Chaos-based cryptography: theory, algorithms and applications (Vol. 354). Springer Science & Business Media.
19. Kocher P, Jaffe J, Jun B (1999) Differential power analysis. In: Advances in cryptology—CRYPTO'99, pp 789–789 Springer
20. Lee TF (2013) An efficient chaotic maps-based authentication and key agreement scheme using smartcards for telecare medicine information systems. J Med Syst 37(6):9985
21. Lee TF, Chang IP, Lin TH, Wang CC (2013) A secure and efficient password-based user authentication scheme using smart cards for the integrated epr information system. J Med Syst 37(3):9941
22. Li CT, Lee CC, Weng CY, Chen SJ (2016) A secure dynamic identity and chaotic maps based user authentication and key agreement scheme for e-healthcare systems. J Med Syst 40(11):233
23. Lovis C, Baud RH, Scherrer J-R (1998) Internet integrated in the daily medical practice within an electronic patient record. Comput Biol Med 28(5):567–579
24. Lu Y, Li L, Peng H, Xie D, Yang Y (2015) Robust and efficient biometrics based password authentication scheme for telecare medicine information systems using extended chaotic maps. J Med Syst 39(6):65
25. Madhusudhan R, Mittal R (2012) Dynamic id-based remote user password authentication schemes using smart cards: a review. J Netw Comput Appl 35(4):1235–1248
26. Masuda N, Aihara K (2002) Cryptosystems with discretized chaotic maps. IEEE Trans Circ Syst I Fundam Theory Appl 49(1):28–40
27. Meingast M, Roosta T, Sastry S (2006) Security and privacy issues with health care information technology. In: 28th annual international conference of the IEEE Engineering in Medicine and Biology Society, 2006. EMBS'06, IEEE, pp 5453–5458
28. Messerges TS, Dabbish EA, Sloan RH (2002) Examining smart-card security under the threat of power analysis attacks. IEEE Trans Comput 51(5):541–552
29. Mir O, van der Weide T, Lee CC (2015) A secure user anonymity and authentication scheme using avispa for telecare medical information systems. J Med Syst 39(9):89
30. Mishra D (2015) On the security flaws in id-based password authentication schemes for telecare medical information systems. J Med Syst 39(1):154
31. Mishra D, Mukhopadhyay S, Kumari S, Khan MK, Chaturvedi A (2014) Security enhancement of a biometric based authentication scheme for telecare medicine information systems with nonce. J Med Syst 38(5):41

32. Mishra D, Srinivas J, Mukhopadhyay S (2014) A secure and efficient chaotic map-based authenticated key agreement scheme for telecare medicine information systems. J Med Syst 38(10):120
33. Moon J, Choi Y, Kim J, Won D (2016) An improvement of robust and efficient biometrics based password authentication scheme for telecare medicine information systems using extended chaotic maps. J Med Syst 40(3):70
34. Nikooghadam M, Zakerolhosseini A (2012) Secure communication of medical information using mobile agents. J Med Syst 36(6):3839–3850
35. Rind DM, Safran C (1993) Real and imagined barriers to an electronic medical record. In: Proceedings of the annual symposium on computer application in medical care, p 74 American medical informatics association
36. Safran C, Goldberg H (2000) Electronic patient records and the impact of the internet. Int J Med Inform 60(2):77–83
37. Shen J, Gui Z, Ji S, Shen J, Tan H, Tang Y (2018) Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. J Netw Comput Appl 106:117–123
38. Steward M (2005) Electronic medical records: privacy, confidentiality, liability. J Leg Med 26(4):491–506
39. Tang PC, Ash JS, Bates DW, Overhage JM, Sands DZ (2006) Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. J Am Med Inform Assoc 13(2):121–126
40. Tsai CS, Lee CC, Hwang MS (2006) Password authentication schemes: Current status and key issues. IJ Netw Secur 3(2):101–115
41. Uslu AM, Stausberg J (2008) Value of the electronic patient record: an analysis of the literature. J Biomed Inf 41(4):675–682
42. van Ginneken AM (2002) The computerized patient record: balancing effort and benefit. Int J Med Inf 65(2):97–119
43. Wang J, Han K, Alexandridis A, Zilic Z, Pang Y, Lin J (2018) An asic implementation of security scheme for body area networks. In: 2018 IEEE International Symposium on Circuits and Systems (ISCAS), IEEE, pp 1–5
44. Wang J, Han K, Alexandridis A, Zilic Z, Pang Y, Wu W, Din S, Jeon G (2018) A novel security scheme for body area networks compatible with smart vehicles. Comput Netw 143:74–81
45. Wazid M, Das AK, Kumar N, Conti M, Vasilakos AV (2018) A novel authentication and key agreement scheme for implantable medical devices deployment. IEEE J Biomed Health Inf 4:22
46. Wei J, Hu X, Liu W (2012) An improved authentication scheme for telecare medicine information systems. J Med Syst 36(6):3597–3604
47. Wen F (2014) A more secure anonymous user authentication scheme for the integrated epr information system. J Med Syst 38(5):42
48. Wen F, Guo D (2014) An improved anonymous authentication scheme for telecare medical information systems. J Med Syst 38(5):26
49. William S (1999) Cryptography and network security: principles and practice. Prentice-Hall, Inc, 23-50
50. Wu F, Xu L (2013) Security analysis and improvement of a privacy authentication scheme for telecare medical information systems. J Med Syst 37(4):9958
51. Wu ZY, Chung Y, Lai F, Chen TS (2012) A password-based user authentication scheme for the integrated epr information system. J Med Syst 36(2):631–638
52. Wu ZY, Lee YC, Lai F, Lee HC, Chung Y (2012) A secure authentication scheme for telecare medicine information systems. J Med Syst 36(3):1529–1535
53. Xie Q, Zhang J, Dong N (2013) Robust anonymous authentication scheme for telecare medical information systems. J Med Syst 37(2):9911
54. Zhang L (2008) Cryptanalysis of the public key encryption based on multiple chaotic systems. Chaos, Solitons & Fractals 37(3):669–674
55. Zhu Z (2012) An efficient authentication scheme for telecare medicine information systems. J Med Syst 36(6):3833–3838

R. Madhusudhan received his M.Tech Degree in 2003 from NITK Surathkal, (A Deemed University) and PhD from IIT Roorkee in 2013. He is currently an Associate Professor in the department of Mathematical and Computational Sciences at NITK, Surathkal, India. He teaches several courses such as Computer Networks, Internet Technology and applications, Database Management Systems. He is life member of Computer Society of India and Indian Society for Technical Education. He is also a member of ACM and IEEE. His current research includes network security, remote user authentication and mobile computation.

Chaitanya S. Nayak received her M.Sc. degree in Mathematics in 2014. Presently she is a research scholar in the Department of Mathematical and Computational Sciences at NITK, Surathkal. Her research is focused on remote user authentication and network security.