Int. j. inf. tecnol. (August 2023) 15(6):3211–3227
https://doi.org/10.1007/s41870-023-01314-7

ORIGINAL RESEARCH

A provably lightweight mutually authentication and key establishment protocol using extended chaotic map for telecare medicine information system

Ashish Kamble[1] · **Vishesh Gaikwad**[1] · **Jitendra Tembhurne**[1]

Received: 3 January 2023 / Accepted: 24 May 2023 / Published online: 24 June 2023

Abstract Telecare Medicine Information System (TMIS) provides patient's efficient and convenient e-healthcare services where the patient private health related information is stored in TMIS server. However, it has also resulted a major privacy and security concerns. Thus, by considering privacy preserving and user anonymity, a major concern, a secure mutual authentication and key establishment protocol needed for creating a secure connection between patients and medical TMIS servers. In research we found major security flaws in already existing authentication schemes. To ensure user anonymity, we propose an efficient, provably secure, lightweight mutually authentication and key establishment protocol using extended chaotic map for TMIS. As the unpredictable behavior of extended chaotic map can provide a possible security solution, a contemporary cryptography. For security and correctness proof of the proposed authentication protocol, BAN (Burrows–Abadi–Needham) logic is adopted. Furthermore, the proposed authentication protocol is secure against various well-known attacks which is proved by formal and informal security analysis. The AVISPA (Automated validation of internet security protocols and application) is utilized to test the correctness of the proposed authentication protocol. Moreover, the proposed protocol satisfies the most required security requirements, with less communication and computation overhead, and outperforms the other existing authentication techniques in terms of computation, communication, storage overheads, and security.

Keywords Telecare medical information system · Authentication · Chaotic Hash function · Extended chaotic map · Random oracle · AVISPA

✉ Jitendra Tembhurne
jtembhurne@iiitn.ac.in

Ashish Kamble
jrfcseashish@iiitn.ac.in

Vishesh Gaikwad
vgaikwad@iiitn.ac.in

[1] Indian Institute of Information Technology, Nagpur, India

1 Introduction

In E-healthcare services like TMIS, we may reduce the time-consuming process such as visiting hospitals, getting medical practitioners' appointment, waiting in queue for a long time, and so on [1, 2]. Since, the introduction of the Internet and communication technologies, internet-based applications became popular and convenient means for consumers to access services from any location. E-healthcare apps are now available for various medical services such as telemedicine, ambulance services, patient healthcare services, physician advice, and TMIS. Patient can access health-related information remotely from anywhere across the world with the E-healthcare service. Interaction between patient at home and physicians from hospitals is feasible via a public communication channel. Because medical data, like electronic health records are transmitted through a public network, an adversary may intercept it. Thus, medical data can be eavesdropped, modified, deleted, and diverted by an enemy. As a result, preserving patient private information from a potential attacker requires an extreme level of confidentiality. Furthermore, the COVID-19 phase [3] is causing problems in several countries across the world. An intelligent method such as TMIS is used widely all over the world. There are some common problems like denial of service (DoS) from the TMIS server, since many patients can use the TMIS server simultaneously, so to protect patient's electronic medical health records and data security for the E-healthcare system is the critical issue. Only authenticated TMIS users, such as patients, physicians, and healthcare staff, may access these services, requiring a robust authentication system. The correct session key exchange techniques are necessary for the user's authenticity to be confirmed. Moreover, authentication tokens such as smartcards, passwords, and biometrics are utilized to validate a specific user. Thus, the resilient scheme should have the following characteristics:

1. A secure authentication and login process.
2. Resistant to password guessing and replay attacks.
3. Authentication is required for both the patient and the authentication server.
4. Agreement and validation of the session key.
5. The cost of communication, processing, and storage must be kept to a minimum.

The uniqueness of biometric keys (such as fingerprints, faces, iris, hand geometry, and palm prints) increases their use in authentication procedures [4]. These keys aid in identifying the proper user and improving authentication protocol security.

The biometric keys provide many benefits that have received a great deal of research are as follows;

1. No need to remember biometric keys.
2. Forging biometric keys is exceedingly challenging.
3. Biometric keys keep their uniqueness.
4. Biometric keys are difficult to guess.

Only the TMIS medical server should be trusted, and no internal user of the medical server should be able to predict the user's password or identity. The Password update phase might be helpful, if the patient chooses to refresh their password. We know that RSA and Elliptic Curve Cryptography (ECC) provide the same level of security. ECC, on the contrary is better suited than RSA because it uses two techniques. One is used to multiply an ECC point by a scalar, while the other is used to add two points on the Elliptic curve, whereas RSA only allows exponentiation [5]. ECC provides a key that is just 160 bits long, whereas RSA uses a key that is 1024 bits long and takes longer to generate than ECC. The hash function and ECC processes are utilized to provide a user authentication mechanism for login. Furthermore, the chaotic map operation is much more efficient and effective of computing than ECC and RSA [6–9], making it accurately adapted for developing a mutual authentication scheme. According to [10], RSA and ECC are the most suitable algorithm for mobile devices where the power is an issue also they have applied simplified Swarm Optimization and Particle Swarm Optimization techniques to Enhance RSA and ECC performance. In [11], states that a mix of provably secure elliptic curves with cyclotomic points and elliptic curves combined with encryption provides increased security. By establishing a connection between an elliptic curve's coordinate and a variable in the polynomial, it leverages the Weierstrass form of an elliptic curve and cyclotomic polynomial to construct a structure. Thus, we can conclude, RSA and ECC both are useful for TMIS services.

As shown in Fig. 1 the architecture of TMIS, patient sharing their medial information with the TMIS medical Server, Physician can access this critical patient information via a public channel, moreover, an attacker is also shown in this system. Patients connect to the medical server using their smartcards from a distance. The smartcard is lightweight and portable at a low cost. The accused of stealing smartcard attack, on either hand, is a significant security flaw in the smartcard-based user login system since it gives the attacker access to all of the critical data contained on the smartcard. This issue is addressed by using mutual authentication via

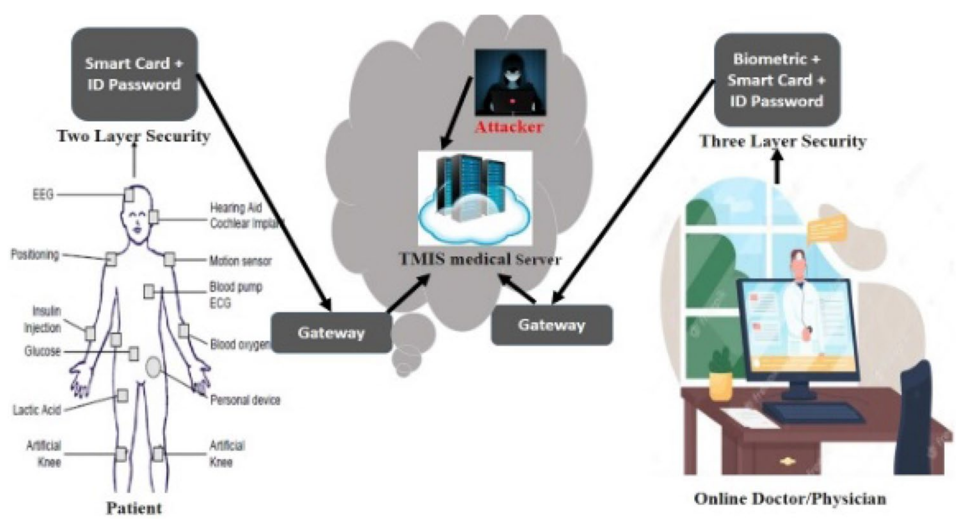


Fig. 1 The architecture of telecare medicine information system

a smartcard. A password guessing vulnerability, in addition to the lost smartcard attack, is a key security problem in smartcard-based authentication systems. Many users are likely to choose weak passwords which can be guessed in polynomial time using virtual memory. To prevent against these known attacks, the authentication protocol masks sensitive data with hash algorithms and XOR operations before storing it in smartcard memory. As a result, the attacker can't read plain messages from the smartcard's memory. Adding biometrics to the login process can improve things even more [12]. Biometric security is improved because it's not feasible to steal, forget, lose, or copy, and impersonate it is exceedingly difficult. Guessing the biometric is also tricky. Authentication and safe data transfer are essential for the remote patient. The password, although being safe, is susceptible to off-line dictionary attacks.

A biometric security system based on fingerprint, iris, retina and a password has been developed to avoid smartcard theft and password guessing attacks. Mutual authentication utilizing both password and user identification is called as two-factor authentication. There are still fewer security vulnerabilities [13–15]. We propose a novel three-factor authentication technique to solve these limitations, which combines a password, identity, and a third element known as biometric to provide utterly safe authentication. This three-factor authentication method is secure against a wide range of security threats.

1.1 Motivation

Due to expensive ECC point multiplication or/and modular exponentiation operations. Extended chaotic map-based user authentication methods are more efficient than ECC or RSA-based schemes, since the key size in Chebyshev chaotic maps is lower than in ECC and RSA. Moreover, we discovered that most chaotic map-based user authentication systems remain vulnerable to several common attacks and cannot offer good user anonymity or smartcard revocation methods [16]. These considerations lead us to propose a low-cost, high-efficiency extended chaotic map-based novel authentication scheme for TMIS server, which will address the security limitations in previous approaches.

1.2 Contributions

Although numerous studies in TMIS security have been published, most of the authentication schemes do not provide maximal security features with minimal computing cost. They are therefore unsuitable for TMIS, i.e., E-healthcare systems.

The main key contributions in this research are as follows:

1. To design a robust security scheme that is resistive against various known security threats.
2. A robust mutual authentication mechanism with key establishment capability is developed to utilize in TMIS.
3. An informal analysis is offered for several security issues of the proposed protocol.
4. The validity of each entity's mutual authentication is proposed using the formal approach BAN logic.
5. Finally, the proposed extended chaotic map authentication scheme for TMIS is compared with several existing schemes.

1.3 Model for attacker

The experimentation of the authentication scheme suggested in this paper occurs via insecure communication. We assume an adversary has the following capabilities. The following are some of the legitimate assumptions:

1. An adversary can access data from a stolen or lost smartcard by monitoring power usage.
2. An enemy can intercept messages sent between entities through a public communication channel.
3. An adversary can alter, resend, and redirect eavesdropped communications.

The organization of this paper is as follows: Related works are discussed in Sect. 2. The characteristics of the Chebyshev chaotic maps, Extended Chaotic map operation, one-way chaotic hash function, and tree-based identity techniques are discussed in Sect. 3. Section 4 explains our user/client authentication scheme for TMIS using one-way chaotic hash, extended chaotic map, and tree-based identity approach. In Sect. 5, presents a various informal and formal security analysis of the proposed authentication scheme. Formal security validation is discussed in Sect. 6. Section 7 highlights the comparison of our authentication scheme with state-of-the-arts. In the last section, we conclude the paper.

2 Related works

In this section, we discuss the existing authentication schemes. In [17], a safe, anonymous authentication mechanism for patients at home is developed. In the same year, the protocol security of [17] is investigated in [18] and discovered that it is two-factor authentication susceptible. To fix the issue, a novel authentication scheme designed for two-factor authentication. In [19], the security aspects of [18] is examined and authors created a password-guess resistant protocol. However, communicating anonymously was not addressed in the developed protocol. Progressively, a secure and efficient lightweight authentication mechanism that protects anonymity in TMIS is proposed in [20]. Further, [21] revealed that identity may be traced in [20] using password and dictionary guesses, in addition to lost/stolen smart card information. Authors, attempted to remove the majority of current threats by developing an anonymous authentication system. Subsequently, authors in [22] revealed that [20] is susceptible to identification and password guessing attacks, in addition to data retrieved from smartcard. As a result, new TMIS system which is more efficient is presented.

In [23], the chaotic map-based authentication mechanism was proposed. Eventually, [24] identified the flaws in [25], the protocol potentially susceptible to stolen smartcards. Further, an effective and secure chaotic map-based authentication protocol and key agreement technique for healthcare was presented in [26]. However, authors in [27] discovered that the system is susceptible to password guessing, impersonation, and impersonation-related attacks. In [28], authors investigated the security breaches in [20], and authentication protocol is vulnerable to password guessing, identity guessing, and stolen/lost smartcard attacks and further presented a TMIS RSA-based authentication technique. Moreover, another TMIS authentication system is proposed in [29]. Leveraging extended chaotic maps, [30] create a trustworthy and efficient certificate-based authentication scheme solution for HIPAA privacy/security rules. In [31], an authentication method based on a verifiably secure Chebyshev chaotic map (CCM) is proposed. This method converted the standard Chebyshev chaotic map key pair into a private key and merged two private keys to create a one-time key that was utilized to encrypt authentication data. A key agreement method is proposed in [32] wherein ECC is utilized for smart grid authentication. Here, the concept of bi-linear paring is not applied, results are verified on ProVerif. Further, light weight ECC is adopted to provide secure communication for smart healthcare under IoT enabled medical system in [33]. The system compatibility can be realized for real time scenario by implementing on suitable hardware.

According to [34], image watermarking is a potential tool for protection, content authentication, fingerprinting, and intellectual property protection. These watermarking techniques may also be more effective for TMIS. The proposed scheme in [35] adopts a dynamic authentication key agreement strategy to preserve the privacy and security of the IoT sensing data that is distributed among the sensors collected by users in the Industrial Internet of Things (IIoT) infrastructure domain, allowing authenticated users to access the data that is distributed among various IoT sensing devices.

A secure 3-factor authentication solution for healthcare services is developed in [36]. Further, [37] examined the protocol's security of [27] and found it vulnerable to password guessing, identity guessing, impersonation, and stolen smartcards attacks. In [38], an efficient, provably secure verifier-based 3-party authentication technique that uses partial discrete logarithm (PDL) to exchange data in TMIS is proposed. This technique does not utilize any server's public keys and requires additional messages and numbers for key confirmation rounds. Moreover, a novel RSA-based authentication technique is proposed in [39]. However, it relies on modulo operations, reducing the protocol's performance due to expensive modulo exponentiation. We present some comparative analysis in terms of security features in Table 1.

3 Preliminaries

In this section, we study Chebyshev chaotic maps and Chebyshev polynomial maps since they will be utilized in the suggested approach. The notations utilized for the scheme are shown in Table 2.

3.1 Chebyshev chaotic maps

We extend on the function of Chebyshev polynomials [44] in this paper. In a variant x, a polynomial (x) is a Chebyshev polynomial with a degree k. Let us consider the exponent x and $x \in [-1, 1]$, as well as the integer n. The polynomial Chebyshev is defined as $(x) = \cos(k \times \arccos(x))$, $\mathscr{T}_{0(x)} = 1$, $\mathscr{T}_{1(x)} = \mathrm{x}, .., \mathscr{T}k_{(x)} = 2x\mathscr{T}k_{-1(x)} - \mathscr{T}k_{-2(x)}; k \geq 2$.

The trigonometric [45] functions $cos(x)$ and $arcos(x)$ are defined as $arcos$: $[-1, 1] \rightarrow [0, \pi]$ and cos: $\mathscr{R} \rightarrow [-1, 1]$. Chebyshev polynomials e has two important features [46, 47]: chaotic and semi-group properties.

3.2 Chaotic property

$\mathscr{T}k$ represents a Chebyshev polynomial map: $[-1, 1] \rightarrow [-1, 1]$ is a chaotic map of degree $k > 1$ with the exponent density function being $f^*(\mathrm{x}) = 1\ (\pi\sqrt{1 - x2})$ and a positive Lyapunov exponent $\lambda = \mathrm{In}\ k > 0$.

3.3 Semi-group property

$\mathscr{T}_{\ell}(\mathscr{T}_{\mathrm{w(z)}}) = \cos\ (\ell\ \cos - 1(\cos(w\cos - 1(x)))) = \cos(\ell w \cos - 1(x)) = \mathscr{T}_{\mathrm{wl(z)}} = \mathscr{T}_{w}(\mathscr{T}_{\mathrm{l(z)}})$, where w and ℓ are positive integers and $x \in [-1, 1]$. Chebyshev polynomials have two main issues, both of which are difficult to solve in polynomial time:

1. DL's (Discrete Logarithms) goal is to find an integer w for which the aim is $(x) = y$for two known components x and y.
2. The goal of DHP (Diffie-Hellman problem's) task is to the estimation of exponent $\mathscr{T}_{\mathrm{l(z)}}$ for three known components x, $\mathscr{T}_{\mathrm{w(z)}}$ and $\mathscr{T}_{\mathrm{l(z)}}$.

Table 1 Comparison of existing schemes

References	Strength	Weakness	Remark and methodology
[26]	To prevent illegal intrusions To protect the usage of a lost or stolen smart card	User impersonation is a threat that can be exploited Server impersonation attack Security to session key	BAN, chaotic maps,
[40]	Password guess attack, Users impersonation attack Smartcard stolen attack Replaying attack Phases of session key recovery and password change	The technique is vulnerable to a password guess attack that occurs off-line It's a privileged insider attack which also has an identity issue	RSA
[41]	It proposes a safe and efficient authentication solution for the integrated EPR information system Does not necessitate the usage of verification tables to store user credentials	There are three key problems in the method, including design faults in the password change step a failure to defend against privileged insider attacks It doesn't have a proper security check	XOR, hash operations
[4]	Biometric-based authentication scheme Off-line password guessing attack	The suggested methodology could not only promptly identify invalid inputs during the login and password changing stages It has the potential could render a lost or stolen smart card useless in the future	Bio hashing, XOR, Hash
[42]	Impersonation attack Stolen smart card attack Privileged insider attack	It does not achieve an efficient Password update phase	Biometric Authentication Scheme, Chaotic map
[43]	User impersonation attack Server impersonation attack	Offline password guess attack Man in middle attack	Elliptic curve cryptography
[26]	Proposed a robust scheme using chebyshev polynomial Off-line password guess attack Stolen verifier	User impersonation attack Server impersonation attack Man in the middle attack	Chaotic map, BAN
[39]	Proposed RSA-based authentication scheme User/Server 's Impersonation attack Man in middle attack	Privilege insider attack	RSA, Random Oracle
[29]	Proposed biometric-based authentication key agreement scheme Perfect forward secrecy User/Server 's Impersonation attack	User anonymity Off-line password guess attack	Chaotic map

Table 2 The notation used in the proposed authentication scheme

Symbol	Description	Symbol	Description
$\mathscr{T}$	Chebyshev chaotic maps	β	Random number by Server (S)
Client $\mathscr{C}_i$	User/ Client /Patient/ Doctor	$\mathscr{q}_1$	Large prime number of bit length
$\mathscr{id}_{\mathscr{C}_i}$	User Identification $\mathscr{C}_i$, where $\mathscr{id}_i \in Sup(\mathbb{T})$	$\mathscr{sk}$	Secret Key
$\mathscr{pw}_{\mathscr{C}_i}$	User Password	$\mathscr{p}_1$	Large prime factors of – 1
$bio_{\mathscr{C}_i}$	Bio—hash Value of User $\boldsymbol{U_i}$	γ	Private Key
α	Random number by SC	v	Public Key
SC	Smart Card	κ_1	Random Number
$\mathscr{S}_j$	Server/Medical Server	$\mathscr{u} \| \mathscr{v}$	and concatenation
$\mathscr{h}_\varsigma$	One way chaotic hash Secure and collision-free one-way chaotic hash function	$\oplus$	Logical XOR operation

3.4 Extended chaotic maps

Zhang et al. [48] demonstrated that the semigroup condition holds for chebyshev polynomials in the interval $(-\infty, +\infty)$.

$((x)) = (2x\mathcal{T}_{k-1(x)} - \mathcal{T}_{k-2(x)})$ (mod $\wp$) where $k \geq 2$, $x \in (-\infty, +\infty)$, and prime number $\wp$ are all prime numbers.

Now, we may establish the recurrence relations, $\mathcal{T}_{k(z)} = 12\mathcal{T}_{k-1(z)} - \mathcal{T}_{k-2(z)}$d 13), where $\mathcal{T}_{1(x)} = 6$ and $\mathcal{T}_{0(z)} = 1$, where $= 13$. The values of (x) are 1, 6, 6, 1, 6, 6,…, which are created by the recurrence stated before $\mathcal{T} = 3$. Here, [49, 50] is the selected timeframe $\mathcal{T}_{l(z)} \equiv \mathcal{T}_{wl(z)} \equiv \mathcal{T}_w(\mathcal{T}_{l(x)})$ (mod $\wp$).

The improved Chebyshev polynomials can still change under composition, and they still have semigroup properties.

3.5 Chaotic hash function (h_ς)

$$\mathcal{Y}_{i+1} = \begin{cases} \frac{y_i}{\gamma}, \text{if } 0 \leq y_i < \gamma \\ \frac{y_i - \gamma}{0.5-\gamma}, \text{if } \gamma \leq y_i < 0.5 \\ \frac{1-y_i-\gamma}{0.5-\gamma}, \text{if } 0.5 \leq y_i < 1-\gamma \\ \frac{1-y_i}{\gamma}, \text{if } 1-\gamma \leq y_i < 1 \end{cases}$$

Chaotic hash function is one-dimensional and piecewise linear map [38, 51, 52, 53, 54], and [55], where $_i \in [0, 1]$ and $\gamma \in (0, 0.5)$ are the control parameter. The parameter γ in $_{i+1}$ ensures that the map will operate in a chaotic state while using $0 < \gamma < 0.5$. The map's self-transformation is done at [0, 1], using only one parameter γ. The transformation begins with using the chaining variables $_0$ and $_i$, which serve as indicators in a one-way hash method.

3.6 Notations

A lightweight mutually authenticated & key-establishment (AKE) protocol using extended chaotic map for TMIS for fuzzy-entity information sharing. Let's look at how often notations are specified, as they will later be used when we get to the details of our new scheme. For simplicity, $[x, y]$ corresponds to $\{x, x+1, ..., y\}$ and $[x]$ corresponds to n$[1, x]$. For every $id = (id_1, id_2, ..., id_k)$, where id is an identity vector, let $S_{id} = \{id_1, ..., id_k\}$ is the set of (id). The id's location record in a tree is defined by $I_{id} = \{i : id_i \in S_{id}\}$. An identified receiver formulate a subtree related to the tree-based encryption technique [56–59]. id and respective places of receivers are joined into $\mathbb{T}$. The legitimate $\mathbb{T}$ must cover the root node. From this we depict that PKG manages the structure. Similarly, identity set of $\mathbb{T}$ and location indices of $\mathbb{T}$ are expressed by $S_{\mathbb{T}} = \cup_{id \in \mathbb{T}} S_{id}$ and $I_{id} = \{i : id_i \in S_{\mathbb{T}}\}$. The symbolizations here can be expressed as $Sup(id) = \{(id_1, id_2, ..., id_{k'}) : k' \leq k\}$ to indicate the superiority of $id = (id_1, id_2, ..., id_k)$. Subtree $\mathbb{T}$'s predictable receivers are categorized as $Sup(\mathbb{T}) = \cup_{id \in \mathbb{T}} Sup(id)$. We present here the symbolizations that are appropriate for the proposed client authentication scheme based on subtree. Suppose that users are structured as shown in Fig. 2 in a tree structure [52]. The $S_{id} = \{\mathcal{B}, \mathcal{F}\}$ and $I_{id} = \{2, 6\}$ are used to specify a known user with $id = (\mathcal{B}, \mathcal{F})$. The $Sup(id) = \{(\mathcal{B}), (\mathcal{B}, \mathcal{F})\}$, a set is created by the user involving superiors of him/her. When message sent by the data owner to receivers set in a subtree i.e. $\mathbb{T} = \{(\mathcal{A})(\mathcal{B}, \mathcal{F}), (\mathcal{B}, \mathcal{G})\}$. Then, $\mathbb{T}$'s identity set is denoted by $S_{\mathbb{T}} = \{\mathcal{A}, \mathcal{B}, \mathcal{F}, \mathcal{G}\}$, and $\mathbb{T}$'s position indices are represented by $I_{\mathbb{T}} = \{1, 2, 6, 7\}$ whereas superiors of $\mathbb{T}$'s are expressed by $Sup(\mathbb{T}) = \{(\mathcal{A}), (\mathcal{B}), (\mathcal{B}, \mathcal{F}), (\mathcal{B}, \mathcal{G})\}$, we see user agreement towards data owner is conveyed.

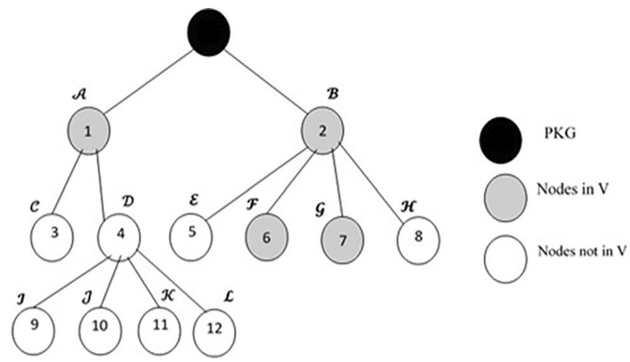


Fig. 2 A Tree-based identity approach authentication scheme representation example

4 Proposed protocol

This section proposes a lightweight mutually authentication and key establishment (AKE) protocol using an extended chaotic map for TMIS. Secure communication between the client and server is a primary concern in the proposed scheme. There are five major phases in the proposed scheme:

Phase 1 (Initial setup phase): TMIS registration center sets up the parameters in off-line mode.

Phase 2 (Client registration phase): Client (Patient/Doctor) gets registered with the registration center (TMIS Server) to avail of the healthcare services.

Phase 3 (Login phase): Client (Patient/Doctor) login takes place to use the TMIS services.

Phase 4 (Authentication phase): TMIS server and client authenticate each other. After authentication, a random session key is generated.

Phase 5 (Password update phase): Legitimate client can update their password. Before updating the password, the client's authenticity needs to be verified.

4.1 Initial setup phase

A large prime $\wp_1$ chooses by the TMIS server and also constructs a prime field $Z^*_{\wp_1}$ and selects his/her private key$\boldsymbol{\beta} \in Z^*_{\wp_1}$. The server defines a function $\hbar_\varsigma : \{0,1\}^* \rightarrow Z^*_{\wp_1}$ as a one-way collision resistant chaotic hash function and a chaotic map $\mathcal{T}$ on $(-\infty, \infty)$ as a Chebyshev polynomial.

$$\mathcal{T}_m(U) = \left[2U\mathcal{T}_{m-1}(U) - \mathcal{T}_{m-2}(U)\right]\left(\bmod q_1\right) for \text{ U} \in (-\infty, \infty)$$

In the proposed system, TMIS user uses fingerprint as a biometric identification. Due to some technical deficiency, sometimes same users' biometric may not match as discussed in [36, 40]. As studied, some pattern matching techniques were developed for such similarity of two biometric authentications of same user. Thus, the system has produced the unique output using pattern matching techniques. From this outstanding output, calculate a Bio-Hash ($bio_{\mathcal{C}_i}$) unique value for the users Client $\mathcal{C}_i$.

4.2 Client registration phase

To obtain the trusted TMIS services, a new client (patient/doctor) need to register themselves as shown in Fig. 3. The registration phase of the AKE (authentication and key establishment) protocol creates a platform for the Client and server to share secret credentials. They can use their optimum privileged credentials during login and authentication to make the computation process more accessible if they share them.

Step RP1: The Client $\mathcal{C}_i$ selects his/her identity ($id_{\mathcal{C}_i} \in Sup(\mathbb{T})$) and password ($pw_{\mathcal{C}_i}$) and computes biometric for Client$\boldsymbol{bio}_{\mathcal{C}_i}$. Additionally, the Client computes,$\mathcal{V}_{ai} = \hbar_\varsigma(pw_{\mathcal{C}_i}||\boldsymbol{bio}_{\mathcal{C}_i})$, $\mathcal{V}_{bi} = \hbar_\varsigma(\boldsymbol{bio}_{\mathcal{C}_i}||id_{\mathcal{C}_i})$ and sends a message $\boldsymbol{M}_0 = \langle \mathcal{V}_{ai}, \mathcal{V}_{bi}\rangle$ using a secure channel.

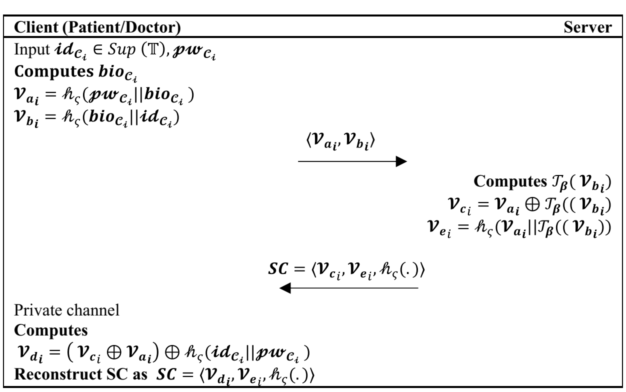


Fig. 3 Registration phase

Step RP2: After receiving the registration message, the server calculates $\mathcal{T}_\beta(\mathcal{V}_{bi})$, $\mathcal{V}_{ci} = \mathcal{V}_{ai} \oplus \mathcal{T}_\beta\left(\mathcal{V}_{bi}\right)$, $\mathcal{V}_{ei} = \hbar_\varsigma(\mathcal{V}_{ai}||\mathcal{T}_\beta((\mathcal{V}_{bi}))$ and fabricate a smartcard with the following details: $\boldsymbol{SC} = \langle \mathcal{V}_{ci}, \mathcal{V}_{ei}, \hbar_\varsigma(.)\rangle$.

In the same private channel, the server sends the smart card $\boldsymbol{SC}$ to the Client (Patient/doctor).

Step RP3: After receiving the smartcard,$\boldsymbol{SC}$, the Client computes $\mathcal{V}_{di} = \left(\mathcal{V}_{ci} \oplus \mathcal{V}_{ai}\right) \oplus \hbar_\varsigma(id_{\mathcal{C}_i}||pw_{\mathcal{C}_i})$ and replaces $\mathcal{V}_{ci}$ with $\mathcal{V}_{di}$ Within the$\boldsymbol{SC}$. Then rebuild the smartcard as$\boldsymbol{SC} = \langle \mathcal{V}_{di}, \mathcal{V}_{ei}, \hbar_\varsigma(.)\rangle$. Figure 3 depicts the entire process involved in the registration procedure.

4.3 Login phase

Before being served, the Client must first login as a legal user. The stages of completing the login procedure are listed below, as prescribed by the scheme. The Client inserted $\boldsymbol{SC}$ into the card reader, followed by his/her $id_{\mathcal{C}_i}, pw_{\mathcal{C}_i}$ and $\boldsymbol{bio}_{\mathcal{C}_i}$. The $\boldsymbol{SC}$ performs calculations,

$$\hbar_\varsigma\left(id_{\mathcal{C}_i}\middle|pw_{\mathcal{C}_i}\right), \mathcal{T}_\beta(\mathcal{V}_{bi}) = \mathcal{V}_{di} \oplus \hbar_\varsigma(id_{\mathcal{C}_i}||pw_{\mathcal{C}_i})$$

$$\mathcal{V}^*_{ai} = \hbar_\varsigma(pw_{\mathcal{C}_i}||\boldsymbol{bio}_{\mathcal{C}_i}), \mathcal{V}^*_{ei} = \hbar_\varsigma(\mathcal{V}^*_{ai}||\mathcal{T}_\beta(pw_{\mathcal{C}_i}||\boldsymbol{bio}_{\mathcal{C}_i}))$$

The smartcard checks to see if the computed $\mathcal{V}^*_{ei}$ is matches to $\mathcal{V}_{ei}$ The one built into the $\boldsymbol{SC}$. The session is terminated, if$\mathcal{V}^*_{ei} \neq \mathcal{V}_{ei}$; otherwise, the $\boldsymbol{SC}$ picks a random integer $\boldsymbol{\alpha}$ and calculates the following:

$$\mathcal{V}_{bi} = \hbar_\varsigma(\boldsymbol{bio}_{\mathcal{C}_i}||id_{\mathcal{C}_i})$$

$$\mathcal{V}_{bi} = \hbar_\varsigma(\boldsymbol{bio}_{\mathcal{C}_i}||id_{\mathcal{C}_i})$$

$$\mathcal{V}_{fi} = \mathcal{T}_\alpha(\mathcal{V}_{bi})$$

$$\mathcal{V}_{gi} = \mathcal{T}_\alpha(\mathcal{T}_\beta(\mathcal{V}_{bi}))$$

$$\mathcal{V}_{gi} = \mathcal{T}_\alpha(\mathcal{T}_\beta(\mathcal{V}_{bi}))$$

$$\mathcal{V}_{hi} = \mathcal{V}_{gi}$$

$$\mathcal{V}_{ji} = \mathcal{V}_{hi} \oplus \mathcal{V}_{ai}$$

$$\mathcal{V}_{ki} = \mathcal{V}_{hi} \oplus \mathcal{V}_{bi}$$

$\mathscr{h}_{\varsigma}(\mathscr{V}_{gi}||\boldsymbol{TS}_1)$

As a login message, the smartcard sends, $M_1 = \langle \mathscr{V}_{fi}, \mathscr{V}_{ji}, \mathscr{V}_{ki}\, \mathscr{V}_{ei}, \boldsymbol{TS}_1, \mathscr{h}_{\varsigma}(\mathscr{V}_{gi}||\boldsymbol{TS}_1)\rangle$ to the medical server, where $\boldsymbol{TS}_1$ is the present time-stamp at the Client.

4.4 Authentication and key generation phase

The TMIS server verifies whether $\left(TS_2 - TS_1\right) < \Delta TS$, where TS_2 is the current server time-stamp and ΔTS is the allowed time delay. The server computes if the time delay is acceptable, $\mathscr{V}^*_{gi} = \mathscr{T}_{\beta}\left(\mathscr{V}_{fi}\right), \mathscr{h}_{\varsigma}(\mathscr{V}^*_{gi}||\boldsymbol{TS}_1)$ & checks if the computed $\mathscr{h}_{\varsigma}(\mathscr{V}^*_{gi}||\boldsymbol{TS}_1)$ is equal as the obtained $\mathscr{h}_{\varsigma}(\mathscr{V}_{gi}||\boldsymbol{TS}_1)$. If $\mathscr{h}_{\varsigma}(\mathscr{V}^*_{gi}||\boldsymbol{TS}_1) \neq \mathscr{h}_{\varsigma}(\mathscr{V}_{gi}||\boldsymbol{TS}_1)$, otherwise, the server terminates the session, $\mathscr{S}_{,}$ picks a random integer γ and computes the following:

$$\mathscr{V}^*_{hi} = \mathscr{V}^*_{gi} \oplus \mathscr{V}_{fi}$$

$$\mathscr{V}^*_{ai} = \mathscr{V}^*_{hi} \oplus \mathscr{V}_{ji}$$

$$\mathscr{V}^*_{bi} = \mathscr{V}^*_{hi} \oplus \mathscr{V}_{ki}$$

$$\mathscr{V}^*_{li} = \mathscr{T}_{\gamma}\left(\mathscr{V}_{bi}\right)$$

$$\mathscr{V}_{mi} = \mathscr{V}^*_{gi} \oplus \mathscr{V}_{li}$$

$$\mathscr{V}_{ni} = \mathscr{V}^*_{ai} \oplus \mathscr{V}_{li}$$

$$\mathscr{h}_{\varsigma}(\mathscr{V}_{mi}||\boldsymbol{TS}_2)$$

The message $M_2 = \langle \mathscr{V}_{ni}, \boldsymbol{TS}_2, \mathscr{h}_{\varsigma}(\mathscr{V}_{mi}||\boldsymbol{TS}_2)\rangle$ is then sent to the Client by the server. When the Client receives the server's response message, he checks if $\left(TS_3 - TS_2\right) < \Delta TS$, where TS_3 is the current time-stamp on the client-side. If it's acceptable, the SC calculates:

$$\mathscr{V}_{ai} = \mathscr{h}_{\varsigma}(\mathscr{pw}_{\mathscr{C}_i}||\boldsymbol{bio}_{\mathscr{C}_i})$$

$$\mathscr{V}'_{li} = \mathscr{V}_{ni} \oplus \mathscr{V}_{ai}$$

$$\mathscr{V}'_{mi} = \mathscr{V}_{gi} \oplus \mathscr{V}'_{li}, \mathscr{h}_{\varsigma}(\mathscr{V}'_{mi}||\boldsymbol{TS}_2)$$

The smart card also double-checks that the computed $\mathscr{h}_{\varsigma}(\mathscr{V}'_{mi}||\boldsymbol{TS}_2)$ matches the obtained $\mathscr{h}_{\varsigma}(\mathscr{V}'_{mi}||\boldsymbol{TS}_2)$. If matched i.e. $\mathscr{h}_{\varsigma}(\mathscr{V}'_{mi}||\boldsymbol{TS}_2) \neq \mathscr{h}_{\varsigma}(\mathscr{V}'_{mi}||\boldsymbol{TS}_2)$ then the shared session key is computed as $\mathscr{sk} = \mathscr{h}_{\varsigma}(\mathscr{V}_{hi}||\mathscr{V}_{li}||\mathscr{V}_{mi}||\mathscr{V}_{gi})$ at the completion of this proper mutual authentication procedure on both sides. As a result, both the client and the server may now communicate via $\mathscr{sk}$. As shown in Fig. 4, the step-by-step calculations with communications involved in both the login and authentication phases is presented.

4.5 Password update phase

It's very likely that the client's password has poor entropy and is easily broken in real time world. In one example, the user could register without having to redo the process. The user can make use of this feature during the password update phase process. Our scheme's safe password updating method is as follows:

The client puts $\boldsymbol{SC}$ into the terminal and inputs the following information: $\mathscr{id}_{\mathscr{C}_i}$, old $\mathscr{pw}_{\mathscr{C}_i}$, *and* $\boldsymbol{bio}_{\mathscr{C}_i}$. The $\boldsymbol{SC}$ calculates $\mathscr{h}_{\varsigma}(\mathscr{id}_{\mathscr{C}_i}||\mathscr{pw}_{\mathscr{C}_i})$, $\mathscr{T}_{\beta}(\mathscr{V}_{bi}) = \mathscr{V}_{di} \oplus \mathscr{h}_{\varsigma}(\mathscr{id}_{\mathscr{C}_i}||\mathscr{pw}_{\mathscr{C}_i})$, $\mathscr{V}^*_{ai} = \mathscr{h}_{\varsigma}(\mathscr{pw}_{\mathscr{C}_i}||\boldsymbol{bio}_{\mathscr{C}_i})$, and $\mathscr{V}^*_{ei} = \mathscr{h}_{\varsigma}(\mathscr{V}^*_{ai}||\mathscr{T}_{\beta}(\mathscr{pw}_{\mathscr{C}_i}||\boldsymbol{bio}_{\mathscr{C}_i}))$. The smart card checks if the calculated $\mathscr{V}^*_{ei} = \mathscr{V}_{ei}$ stored in server(S). The session is canceled if $\mathscr{V}^*_{ei} \neq \mathscr{V}_{ei}$; otherwise, the S requests the Client to provide a new password. The user enters the new password $\mathscr{pw}^{new}_{\mathscr{C}_i}$ In response to the $\boldsymbol{SC}$ command. Following new values are calculated by the smart card.

$\mathscr{V}^{new}_{ai} = \mathscr{h}(\mathscr{pw}^{new}_{\mathscr{C}_i}||\boldsymbol{bio}_{\mathscr{C}_i})$, $\mathscr{V}^{new}_{ci} = (\mathscr{V}_{ci} \oplus \mathscr{V}_{ai} \oplus \mathscr{V}^{new}_{ai})$, $\mathscr{V}^{new}_{ei} = \mathscr{h}_{\varsigma}(\mathscr{V}^{new}_{ai}||\mathscr{T}_{\beta}(\mathscr{V}_{bi}))$, and $\mathscr{V}^{new}_{di} = (\mathscr{V}^{new}_{ci} \oplus \mathscr{V}^{new}_{ai}) \oplus \mathscr{h}_{\varsigma}(\mathscr{pw}^{new}_{\mathscr{C}_i}||\mathscr{id}_{\mathscr{C}_i})$. Replaces the old $\mathscr{V}_{di}$ and $\mathscr{V}_{ei}$ with the new $\mathscr{V}^{new}_{di}$ *and* $\mathscr{V}^{new}_{ei}$ within the smartcard. $\mathscr{V}_{di}$ and $\mathscr{V}_{ei}$ are two variables. Figure 5 depicts the full procedure of changing the password.

5 Security analysis of the proposed protocol

The proposed protocol security is critical in terms of implementation. Our protocol's security analysis is divided into three sub sections. Informal security analysis for different security threats, Formal security analysis utilizing BAN logic for mutually authenticated and key-agreement and Formal verification using AVISPA simulation tool.

5.1 Informal security analysis

In this subsection, many of the essential security threats and common security features are discussed informally.

Theorem 1 *The suggested protocol can resist an off-line identification guessing threat.*

Fig. 4 Login and Authentication phase

User Patient/Doctor $U/_{SC} = \langle \mathcal{V}_{d_i}, \mathcal{V}_{e_i}, \hbar_\varsigma(.) \rangle$ **Server**

Input $id_{\mathcal{C}_i}, pw_{\mathcal{C}_i}$ *and* $bio_{\mathcal{C}_i}$

SC **Computes** $\hbar_\varsigma(id_{\mathcal{C}_i} || pw_{\mathcal{C}_i})$

$\mathcal{T}_\beta(\mathcal{V}_{b_i}) = \mathcal{V}_{d_i} \oplus \hbar_\varsigma(id_{\mathcal{C}_i} || pw_{\mathcal{C}_i})$

$\mathcal{V}_{a_i}^* = \hbar_\varsigma(pw_{\mathcal{C}_i} || bio_{\mathcal{C}_i})$

$\mathcal{V}_{e_i}^* = \hbar_\varsigma(\mathcal{V}_{a_i}^* || \mathcal{T}_\beta(pw_{\mathcal{C}_i} || bio_{\mathcal{C}_i}))$

Checks $\mathcal{V}_{e_i}^* = \mathcal{V}_{e_i}$

Generates a random α

Computes

$\mathcal{V}_{b_i} = \hbar_\varsigma(bio_{\mathcal{C}_i} || id_{\mathcal{C}_i})$

$\mathcal{V}_{f_i} = \mathcal{T}_\alpha(\mathcal{V}_{b_i})$

$\mathcal{V}_{g_i} = \mathcal{T}_\alpha(\mathcal{T}_\beta(\mathcal{V}_{b_i}))$

$\mathcal{V}_{h_i} = \mathcal{V}_{g_i}$

$\mathcal{V}_{j_i} = \mathcal{V}_{h_i} \oplus \mathcal{V}_{a_i}$

$\mathcal{V}_{k_i} = \mathcal{V}_{h_i} \oplus \mathcal{V}_{b_i}$

$\hbar_\varsigma(\mathcal{V}_{g_i} || TS_1)$

$M_1 = \langle \mathcal{V}_{f_i}, \mathcal{V}_{j_i}, \mathcal{V}_{k_i} \mathcal{V}_{e_i}, TS_1, \hbar_\varsigma(\mathcal{V}_{g_i} || TS_1) \rangle$ →

Checks $(TS_2 - TS_1) < \Delta TS$

Computes $\mathcal{V}_{g_i}^* = \mathcal{T}_\beta(\mathcal{V}_{f_i})$

$\hbar_\varsigma(\mathcal{V}_{g_i} || TS_1)$

Checks

$\hbar_\varsigma(\mathcal{V}_{g_i}^* || TS_1) = \hbar_\varsigma(\mathcal{V}_{g_i} || TS_1)$

Selects a random γ

Computes

$\mathcal{V}_{h_i}^* = \mathcal{V}_{g_i}^* \oplus F_i$

$\mathcal{V}_{a_i}^* = \mathcal{V}_{h_i}^* \oplus \mathcal{V}_{j_i}$

$\mathcal{V}_{b_i}^* = \mathcal{V}_{h_i}^* \oplus \mathcal{V}_{k_i}$

$\mathcal{V}_{l_i}^* = \mathcal{T}_\gamma(\mathcal{V}_{b_i})$

$\mathcal{V}_{m_i} = \mathcal{V}_{g_i}^* \oplus \mathcal{V}_{l_i}$

$\mathcal{V}_{n_i} = \mathcal{V}_{a_i}^* \oplus \mathcal{V}_{l_i}$

$\hbar_\varsigma(\mathcal{V}_{m_i} || TS_2)$

← $M_2 = \langle \mathcal{V}_{n_i}, TS_2, \hbar_\varsigma(\mathcal{V}_{m_i} || TS_2) \rangle$

Checks

$(TS_2 - TS_1) < \Delta TS$

Computes

$\mathcal{V}_{a_i} = \hbar_\varsigma(pw_{\mathcal{C}_i} || bio_{\mathcal{C}_i})$

$\mathcal{V}_{l_i}' = \mathcal{V}_{n_i} \oplus \mathcal{V}_{a_i}$

$\mathcal{V}_{m_i}' = \mathcal{V}_{g_i} \oplus \mathcal{V}_{l_i}'$

$\hbar_\varsigma(\mathcal{V}_{m_i}' || TS_2)$

Checks $\hbar_\varsigma(\mathcal{V}_{m_i}' || TS_2) = \hbar_\varsigma(\mathcal{V}_{m_i}' || TS_2)$

$sk = \hbar_\varsigma(\mathcal{V}_{h_i} || \mathcal{V}_{l_i} || \mathcal{V}_{m_i} || \mathcal{V}_{g_i})$

Proof As the client uses several methods of maintaining and remembering separate identities for different application unnecessarily. For the sake of ease, user might typically uses the same identity across many applications. According to the adversary model's premise, the attacker can infer the lower entropy user's identity. The suggested protocol's login request,

$$M_1 = \langle \mathcal{V}_{f_i}, \mathcal{V}_{j_i}, \mathcal{V}_{k_i} \mathcal{V}_{e_i}, TS_1, \hbar_\varsigma(\mathcal{V}_{g_i} || TS_1) \rangle. \tag{1}$$

Here the message (M_1) as shown in (1) of suggested protocol involves users identification $id_{\mathcal{C}_i}$ as shown below.

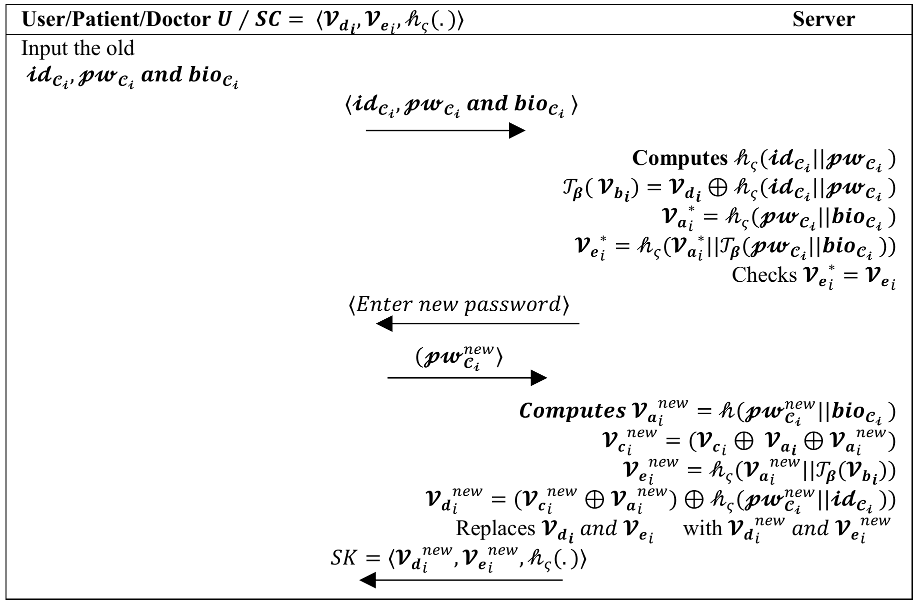
$$\mathcal{V}_{f_i} = \mathcal{T}_\alpha(\mathcal{V}_{bi}) \tag{2}$$

$$\begin{aligned} \mathcal{V}_{ji} &= \mathcal{V}_{hi} \oplus \mathcal{V}_{ai} \\ &= \mathcal{V}_{gi} \oplus \mathcal{V}_{fi} \oplus \hbar_\varsigma(pw_{\mathcal{C}_i} || bio_{\mathcal{C}_i}) \\ &= \mathcal{T}_\alpha\left(\mathcal{T}_\beta\left(\mathcal{V}_{bi}\right)\right) \oplus \mathcal{T}_\alpha\left(\mathcal{V}_{bi}\right) \oplus \hbar_\varsigma(pw_{\mathcal{C}_i} || bio_{\mathcal{C}_i}) \end{aligned} \tag{3}$$

$$\mathcal{V}_{ki} = \mathcal{V}_{hi} \oplus \mathcal{V}_{bi}, \ \mathcal{V}_{ki} = \mathcal{V}_{bi} \oplus \mathcal{T}_\alpha(\mathcal{T}_\beta(\mathcal{V}_{bi})) \oplus \mathcal{T}_\alpha(\mathcal{V}_{bi}) \tag{4}$$

As $\mathcal{V}_{bi} = \hbar_\varsigma(bio_{\mathcal{C}_i} || id_{\mathcal{C}_i})$ is used in the production of all these composite messages. Even if an adversary predicts

Fig. 5 Password update phase



the user identification $id_{\mathscr{C}_i}$, the adversary cannot check and validate his/her claim without knowing $\boldsymbol{bio}_{\mathscr{C}_i}$. Aside from that, other parameter $\boldsymbol{\beta}$ is also hidden. Comparable arguments can apply to the composite message M_2 as well. As a result, the suggested protocol is immune to an off-line identification guessing threat.

Theorem 2 *Our proposed technique is well-protected against off-line password guess attack.*

Proof. In off-line, an attacker might try to determine the user's password and see if his / her attempt is valid. After acquiring the collection of login & authentication messages M_1& M_2 is taken from equation (1) and (6), respectively.

$$M_1 = \langle \mathscr{V}_{f_i}, \mathscr{V}_{j_i}, \mathscr{V}_{ki}\, \mathscr{V}_{ei}, \boldsymbol{TS}_1, h_\varsigma\left(\mathscr{V}_{g_i}||\boldsymbol{TS}_1 \right) \rangle \& M_2 = \langle \mathscr{V}_{ni}, \boldsymbol{TS}_2, h_\varsigma(\mathscr{V}_{mi}||\boldsymbol{TS}_2) \rangle \tag{5}$$

During the session, the attacker can guess the user's password $pw_{\mathscr{C}_i}$. To test his/her theory, assume the attacker looks for the composite message which includes $pw_{\mathscr{C}_i}$. in M_1 and M_2. M_1 composite message containing $pw_{\mathscr{C}_i}, \mathscr{V}_{ji}$ as shown below.

$$\begin{aligned} \mathscr{V}_{ji} &= \mathscr{V}_{hi} \oplus \mathscr{V}_{ai} \\ &= \mathscr{V}_{gi} \oplus \mathscr{V}_{fi} \oplus h_\varsigma(pw_{\mathscr{C}_i}||\boldsymbol{bio}_{\mathscr{C}_i}) \\ &= \mathscr{T}_\alpha\left(\mathscr{T}_\beta\left(\mathscr{V}_{bi}\right)\right) \oplus \mathscr{T}_\alpha\left(\mathscr{V}_{bi}\right) \oplus h_\varsigma(pw_{\mathscr{C}_i}||\boldsymbol{bio}_{\mathscr{C}_i}) \\ &= \mathscr{T}_\alpha(\mathscr{T}_\beta(h_\varsigma(\boldsymbol{bio}_{\mathscr{C}_i}||id_{\mathscr{C}_i}))) \oplus \mathscr{T}_\alpha(h_\varsigma(\boldsymbol{bio}_{\mathscr{C}_i}||id_{\mathscr{C}_i})) \oplus h_\varsigma(pw_{\mathscr{C}_i}||\boldsymbol{bio}_{\mathscr{C}_i}) \end{aligned} \tag{6}$$

& in M_2 is $\mathscr{V}_{ni}$ as

$$\begin{aligned} \mathscr{V}_{ni} &= \mathscr{V}_{ai}^* \oplus \mathscr{V}_{li} = \mathscr{T}_\gamma\left(\mathscr{V}_{bi}^*\right) \oplus \mathscr{V}_{ai}^* \\ &= \mathscr{T}_\gamma\left(\mathscr{V}_{bi}^*\right) \oplus \mathscr{V}_{ai}^* \\ &= T_y(h_\varsigma(\boldsymbol{bio}_{\mathscr{C}_i}||id_{\mathscr{C}_i}) \oplus h_\varsigma(pw_{\mathscr{C}_i}||\boldsymbol{bio}_{\mathscr{C}_i}) \end{aligned} \tag{7}$$

To confirm the correctness of the assumed $pw_{\mathscr{C}_i}$, the adversary has to know the extra secret parameters $\boldsymbol{\alpha}, \boldsymbol{\beta}, \gamma$ and, most importantly, $\boldsymbol{bio}_{\mathscr{C}_i}$. As a result, checking the anticipated $pw_{\mathscr{C}_i}$ in a polynomial-time procedure is computationally challenging. As a result, the suggested authentication technique can survive a password guessing attack off-line.

Theorem 3 *The suggested protocol is resistant to attacks on traceability.*

Proof Because, the attacker can maintain track of a particular user's login messages and thereby harm the user's privacy, the adversary should not be able to determine which login message belongs to which user. Assume an attacker captures any two random login messages $M_1 = \langle \mathscr{V}_{f_i}, \mathscr{V}_{j_i}, \mathscr{V}_{ki}, \boldsymbol{TS}_1, h_\varsigma\left(\mathscr{V}_{g_i}||\boldsymbol{TS}_1 \right) \rangle$ and $M_1^* = \langle \mathscr{V}_{f_i}^*, \mathscr{V}_{j_i}^*, \mathscr{V}_{k_i}^*, \boldsymbol{TS}_1, h_\varsigma(\mathscr{V}_{g_i}^*||\boldsymbol{TS}_1)^* \rangle$ for a certain server, because each composite message includes a session parameter in their composition, the attacker cannot identify any similarities in the composite messages. As a result, the suggested approach can withstand a tracing attack.

Theorem 4 *The suggested protocol is resistant against insider attack.*

Proof It is common for people to use the same user identification and password for their online accounts. An insider on TMIS server may take note of their user's identification and password also utilize them to log in as a genuine user on another server. The user sends the anonymous identity and password $\mathscr{V}_{ai} = \mathscr{h}_{\varsigma}(\mathscr{pw}_{\mathscr{C}_i}||bio_{\mathscr{C}_i})$ & $\mathscr{V}_{bi} = \mathscr{h}_{\varsigma}(bio_{\mathscr{C}_i}||\mathscr{id}_{\mathscr{C}_i})$ to the TMIS server during the (RP) registration phase of our protocol. It is computationally challenging to get $\mathscr{V}_{bi}||\mathscr{id}_{\mathscr{C}_i}$ and $\mathscr{pw}_{\mathscr{C}_i}$ from $\mathscr{V}_{bi}$ and $\mathscr{V}_{ai}$ Because of the features of the 1-way hash function. Furthermore, it is computationally impossible to predict the $\mathscr{id}_{\mathscr{C}_i}$ & $\mathscr{pw}_{\mathscr{C}_i}$ without knowing the hidden value $\mathscr{V}_{bi}$. Consequently, our protocol is impervious to insider threats.

Theorem 5 *The enhanced protocol is strongly protected against user impersonation attacks.*

Proof. If an attacker wants to impersonate a specific user, he/ she must record that user's login message and edit the composite messages as needed. Because our protocol is resistant to traceability attacks, the attacker will not collect a specific user's login message. Assume the attacker is a valid user who intends to mimic another user by constructing the login message, As shown in Eq. (1) a composite message $M_1 = \langle \mathscr{V}_{fi}, \mathscr{V}_{ji}, \mathscr{V}_{ki}, \boldsymbol{TS}_1, \mathscr{h}_{\varsigma}(\mathscr{V}_{gi}||\boldsymbol{TS}_1)\rangle$ generated in his own, in which the value of the secret parameters $\mathscr{id}_{\mathscr{C}_i}, \mathscr{pw}_{\mathscr{C}_i}$ and $\boldsymbol{bio}_{\mathscr{C}_i}$ is desired for the creation of the composite messages $\mathscr{V}_{fi}, \mathscr{V}_{ji}, \mathscr{V}_{ki}$, and $\mathscr{h}_{\varsigma}(\mathscr{V}_{gi})$. The attacker cannot generate the login message M_1 of a specific user even though they are unique to each user. Consequently, the suggested protocol is resilient to the impersonation attack.

Theorem 6 *Our scheme is secure against server impersonation attacks.*

Proof Allow the login message to be captured by an adversary i.e. from Eq. (1), $M_1 = \langle \mathscr{V}_{fi}, \mathscr{V}_{ji}, \mathscr{V}_{ki}, \boldsymbol{TS}_1, \mathscr{h}_{\varsigma}(\mathscr{V}_{gi}||\boldsymbol{TS}_1)\rangle$ and an attacker trying to create response message as shown in Eq. (6), $M_2 = \langle \mathscr{V}_{ni}, \boldsymbol{TS}_2, \mathscr{h}_{\varsigma}(\mathscr{V}_{mi}||\boldsymbol{TS}_2)\rangle$ impersonate as a genuine server, where $\mathscr{V}_{ni}$ and $\mathscr{V}_{mi}$ are as follows: $\mathscr{V}_{mi} = \mathscr{V}^*_{gi} \oplus \mathscr{V}_{li}, \mathscr{V}_{ni} = \mathscr{V}^*_{ai} \oplus \mathscr{V}_{li}, \mathscr{V}_{gi}$ must be used by the attacker to derive $\mathscr{V}_{ai}$ from $\mathscr{V}_{fi}$ and $\mathscr{V}_{ji}$. However, to compute $\mathscr{V}_{gi} = \mathscr{T}_{\beta}\left(\mathscr{V}_{fi}\right)$, the server's secrete parameter s must be known. As a result, without knowing the value of the server's secrete parameter s, the attacker cannot compute $\mathscr{V}_{ni}$ and $\mathscr{V}_{mi}$ As a result, our protocol is resistant to server impersonation attacks.

Theorem 7 *The suggested protocol resilient replaying attack.*

Proof Assume that an adversary tries to execute the replaying attack on the suggested protocol by sending an old login message $M_1 = \langle \mathscr{V}^{old}_{f1}, \mathscr{V}^{old}_{j1}, \mathscr{V}^{old}_{k1}, TS^{old}_1, \mathscr{h}_{\varsigma}(\mathscr{V}_{gi}||TS_1)^{old}\rangle$ to $server(S)$. Because of the old time-stamp T^{old}_1, the server will verify for the time latency $\left(TS_2 - TS_1\right) < \Delta TS$ and fails. Similarly, the time-stamp T^{old}_2 is included in the server responded message, thus old M_2 cannot be replayed. As a result, the suggested protocol is resistant to replaying attacks.

Theorem 8 *The suggested protocol ensures perfect forward secrecy.*

Proof If the previous session keys were compromised, the attacker may be able to decode previously sent messages, exposing the shared secret. Both Client and server compute the session key in the proposed technique at the end of mutual authentication is

$$\mathscr{sk} = \mathscr{h}_{\varsigma}\left(\mathscr{V}_{hi}\middle|\middle|\mathscr{V}_{li}\middle|\middle|\mathscr{V}_{mi}||\mathscr{V}_{gi}\right) \text{in which } \mathscr{V}_{gi} = \mathscr{T}_{\alpha}(\mathscr{T}_{\beta}(\mathscr{V}_{bi})) \tag{8}$$

$$\mathscr{V}_{hi} = \mathscr{V}_{gi} \oplus \mathscr{V}_{fi} \tag{9}$$

$$\mathscr{V}_{hi} = \mathscr{T}_{\alpha}(\mathscr{T}_{\beta}(\mathscr{V}_{bi})) \oplus \mathscr{T}_{\alpha}(\mathscr{V}_{bi}) \tag{10}$$

$$\mathscr{V}_{li} = \mathscr{T}_{\gamma}\left(\mathscr{V}_{bi}\right) \tag{11}$$

$$\mathscr{V}_{mi} = \mathscr{V}_{gi} \oplus \mathscr{V}_{li} = \mathscr{T}_{\alpha}(\mathscr{T}_{\beta}(\mathscr{V}_{bi})) \oplus \mathscr{T}_{\gamma}\left(\mathscr{V}_{bi}\right) \tag{12}$$

Even if the server's longer—term secrets value ($\boldsymbol{\beta}$) is known, the adversary cannot compute our protocol session key $\mathscr{sk} = \mathscr{h}_{\varsigma}(\mathscr{V}_{hi}||\mathscr{V}_{li}||\mathscr{V}_{mi}||\mathscr{V}_{gi})$, since the session random nonce i.e. x&y involve in every composite message transfer as shown in proposed authentication scheme. The session key is dependent on both the server and the user's longer-term secrets and the session secrets. consequently, 100% forward secrecy is achieved by the proposed protocol.

Theorem 9 *Forward secrecy is robust protection against a Stolen verifier attack in the protocol suggested.*

Proof There is no such verifier table is required for verification in our protocol. i.e., throughout the login and authentication procedure, our system doesn't need the use of a verification table. Therefore the absence of a verifier table removes the possibility of a stolen-verifier attack [60].

Theorem 10 *The suggested protocol safe against man in the middle threat.*

Proof Allow an adversary to record a legitimate user's login message $M_1 = \langle \mathscr{V}_{f_i}, \mathscr{V}_{j_i}, \mathscr{V}_{ki}, \boldsymbol{TS}_1, h_\varsigma(\mathscr{V}_{g_i}||\boldsymbol{TS}_1)\rangle$ and tries to come up with a valid M_1^{new} on its own. It is computationally impossible for the adversary to produce a legitimateM_1^{new}, as indicated in the user impersonation attack as proved in theorem 5. Furthermore, if the adversary tries to respond with a genuine login message, it is computationally infeasible to create a responsive message M_2^{new} and persuade the user, as our technique withstands server impersonation attacks. As a result, the suggested protocol is impervious to a man in the middle threat.

5.2 BAN logic is a formal method to prove authentication

BAN logic is initially utilized to test the security protocol's correctness [61]. The BAN logic is a formal approach for determining if a protocol can resist security risks such as replay attacks, eavesdropping, and man-in-the-middle attacks. This formal technique primarily focuses on confirming the message origin, message freshness, and origin's trustworthiness in the security protocol. The BAN logic, with its formal definitions, syntax, and postulates, is well-established for analyzing authentication protocols. The study begins with a BAN logic model of the intended protocol that follows a well-defined syntax. The basic assumptions for the planned procedure are established after the Idealization. The set of objectives to be met is then determined based on the attributes that must be verified. Finally, the idealized procedure is combined with definitions, postulates, and assumptions to meet the needed set of goals can be found in [62, 63].

5.2.1 Idealization of proposed protocol

To do the formal analysis, the suggested authentication scheme must be idealized in BAN logic. The sharing credentials may be discovered since the login message is written in such a way that the user authenticated towards the server. Applying $\mathscr{V}_{f_i}$ the user integrates $\mathscr{V}_{ai}$, $\mathscr{V}_{g_i}$, and masks in the suggested protocol, also in that same message the user combines $\mathscr{V}_{g_i}$ with the time-stamp TS_1.The login message M_1 may be simplified in the BAN logic using this concept. The server combines $\mathscr{V}_{gi}$ with the time-stamp TS_2 in the responsive message and masks it with $\mathscr{V}_{li}$. As a result, these are the idealised messages:

$$M_1 = \langle \mathscr{V}_{f_i}, \langle \mathscr{V}_{ai}, \mathscr{V}_{gi}\rangle_{\mathscr{V}_{f_i}}, \mathscr{V}_{ki}, \langle \mathscr{V}_{gi}\rangle_{TS_1}\rangle$$

$$M_2 = \langle \mathscr{V}_{ni}, \langle \mathscr{V}_{mi}\rangle_{\mathscr{V}_{li}}$$

To do the formal analysis, the suggested system must be idealized in BAN logic. The shared credentials may be discovered since the login message is written so that the patient/client (user) authenticates to the TMIS server. The Client combines $\mathscr{V}_{ai}$, $\mathscr{V}_{g_i}$ and masks using $\mathscr{V}_{f_i}$, in the suggested protocol, and the Client also integrates $\mathscr{V}_{g_i}$ with the time-stamp TS_1 in the same message. The login message M_1 may be idealised in the BAN logic using this concept. The server combines $\mathscr{V}_{g_i}$ with the time-stamp TS_2 in the response message and masks it with $\mathscr{V}_{li}$. As a result, these are the idealised messages:

$$M_1 = \langle \mathscr{V}_{f_i}, \langle \mathscr{V}_{ai}, \mathscr{V}_{gi}\rangle_{\mathscr{V}_{f_i}}, \mathscr{V}_{ki}, \langle \mathscr{V}_{gi}\rangle_{TS_1}\rangle, M_2 = \langle \mathscr{V}_{ni}, \langle \mathscr{V}_{mi}\rangle_{\mathscr{V}_{li}}$$

5.2.2 Security objectives

The users must establish the security objectives according to needed attributes to be validated to properly analyze the proposed technique. To provide mutual authentication between both Client and the TMIS server, we establish the essential security objectives in our protocol.

$$G_1 : S_k| \equiv U_i| \equiv G_i$$

$$G_2 : S_k| \equiv G_i$$

$$G_3 : U_i| \equiv S_k| \equiv M_i$$

$$G_4 : U_i| \equiv M_i$$

$$G_5 : U_i| \equiv U_i \overset{S_k}{\leftrightarrow} S_k$$

$$G_6 : S_k| \equiv U_i \overset{S_k}{\leftrightarrow} S_k$$

The additional objectives G_5, G_6 are established to guarantee that the session key is exchanged solely between the Client and the server, and the security objectives G_1toG_4 certify that the Client and server are mutually authenticated.

5.2.3 Preliminary assumptions

In order to derive the above-mentioned goals, the formal methodology allows the user to make certain basic assumptions based on the given protocol. The first assumptions made regarding the proposed protocol in regard to the defined security goals are listed below.

$$A_1 : S_k| \equiv U_i \overset{F_i}{\leftrightarrow} S_k$$

$A_2 : S_k| \equiv \#x$

$A_3 : S_k| \equiv U_i| \Rightarrow G_i$

$A_4 : U_i| \equiv U_i \overset{L_i}{\leftrightarrow} S_k$

$A_5 : U_i| \equiv \#y$

$A_6 : U_i| \equiv S_k| \Rightarrow L_i$

5.2.4 Scheme analysis

Let us utilize the rule on the message M_1, $ST_1 : S_k \triangleleft \langle F_i, A_i, G_{iF_i}, K_i, \mathscr{A}(G_i||T_1)\rangle$. Simultaneously, with ST_1, we derive $ST_2 : S_k \triangleleft A_i, G_{iF_i}$, using the subcomponent rule of the seeing rule.

By applying assumptions, A_1 on ST_2 and by message meaning rule, we derive $ST_3 : | \equiv U_i \sim \langle A_i, G_i\rangle$. Applying its subcomponent rule, we get $ST_4 : S_k| \equiv U_i| \sim G_i$.

As we have$G_i = T_x(T_s(B_i))$, using the assumption A_2 and freshness rule, we get$ST_5 : S_k| \equiv \#G_i$. Using ST_4 and ST_5 in nonce verification rule, we get $G_1 : S_k \equiv U_i| \equiv G_i.(\boldsymbol{Goal G_1})$. Using G_1 and A_3 in Jurisdiction rule, we get $G_2 : S_k \equiv G_i.(\boldsymbol{Goal G_2})$ According to seeing rule,$ST_6 : U_i \triangleleft \langle N_i, \mathscr{A}(M_i)\rangle$.

As user possesses $A_i, L_i = N_i A_i and M_i = G_i L_i$, we have$ST_7 : U_i \triangleleft \langle N_i, \langle M_i\rangle_{L_i}\rangle$.

Using assumption A_4 and by message meaning rule, we get $ST_8 : U_i| \equiv S_k \sim M_i$. As $M_i = G_i T_Y(B_i)$, using the assumption A_5 and subcomponent rules for freshness, we get $ST_9 : U_i| \equiv \#M_i$.

Using ST_8 and ST_9 in nonce verification rule, we get$G_3 : U_i| \equiv S_k| \equiv M_i.(\boldsymbol{Goal G_3})$. As $M_i = G_i \oplus L_i$ and using assumptionA_6, we get$ST_{10} : U_i| \equiv \#M_i$.

Using ST_{10} and G_3 in Jurisdiction rule, we get$G_4 : U_i| \equiv M_i.(\boldsymbol{Goal G_4})$.

Since, $S_k = \mathscr{A}(\boldsymbol{H_i}||\boldsymbol{L_i}||\boldsymbol{M_i}||\boldsymbol{G_i})$, by using ST_9 with G_3 in the session key rule, we get get$G_5 : U_i| \equiv U_i \overset{SK}{\leftrightarrow} S_k.(\boldsymbol{Goal G_5})$. Similarly, by using ST_5 with G_1 in the session key rule, we get $S_k G_6 : S_k| \equiv U_i \overset{SK}{\leftrightarrow} S_k.(\boldsymbol{Goal G_6})$.

5.3 Formal verification using AVISPA

In this subsection, we utilize the AVISPA for formal verification of the proposed authentication and key exchange protocol. The AVISPA uses role-based programming language i.e., HLPSL (High-Level Protocol Specification Language) programming language [56, 57]. The AVISPA is a well-known tool for verifying that proposed protocols are secure against replay and man-in-the-middle attacks.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/ChaoticmapFinal.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 2.81s
  visitedNodes: 18 nodes
  depth: 4 plies
```

Fig. 6 Final experimental result of the formal security analysis using AVISPA tool generated by OFMC back-end

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/ChaoticmapFinal.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 8 states
  Reachable  : 8 states
  Translation: 0.24 seconds
  Computation: 0.00 seconds
```

Fig. 7 Final Experimental result of the formal security analysis using AVISPA tool generated by CL-AtSe back-end

The following four back-ends can be utilized to implement the AVISPA tool.

1. OFMC (On the Fly Model Checker)
2. CL-AtSe (Constraint Logic based Attack Searcher)

3. TA4SP (Tree Automate Based Protocol Analyzer)
4. SATMC (SAT Based Model Checker).

The AVISPA simulation results of our proposed protocol are as follows. To simulate the our proposed authentication and key exchange protocol, we use the OFMC back-end of the AVISPA tool, as shown in Fig. 6 and CL-AtSe back-end, as shown in Fig. 7. The findings demonstrate that the proposed protocol is safe from passive and active attacks, including replay attacks, man-in-the-middle attacks, and user anonymity attacks, which are all major security issues in TMIS.

6 Performance comparison

This section demonstrated the performance analysis and comparison study related to the security and functionality characteristics offered by the scheme presented. our approach performance will look at storage costs, computational overheads, and communication costs. To accomplish

Table 3 Various attacks

Attacks	[27]	[36]	[39]	[29]	[58]	[59]	[3]	Our
A1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A2	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
A3	No	Yes	Yes	Yes	Yes	No	Yes	Yes
A4	No	Yes	Yes	No	Yes	Yes	Yes	Yes
A5	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
A6	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A7	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A8	No	No	Yes	No	Yes	Yes	No	Yes
A9	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A10	No	No	No	Yes	No	Yes	Yes	Yes
A11	No	No	Yes	Yes	Yes	Yes	Yes	Yes
A12	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Attacks A1: Offline Identity guessing attack, A2: Offline password guessing attack, A3: Traceability attack, A4: Replaying attack, A5: Stolen verifier attack, A6: Users Impersonation attack A7: Server Impersonation attack, A8: Achieves User Anonymity, A9: Mutual Authentication, A10: Privileged insider attack, A11: Perfect Forward secrecy, A12: Man in the middle attack

Table 4 Notations used for computational cost and Execution time for each operation

Notation used	Meaning (Execution time)	In seconds
Th	One way hash function	0.0005
Tccm	Chebyshev chaotic map	0.02102
Tsym	Symmetric key encryption-decryption operation	0.0087
Tecc	One elliptic curve point multiplication	0.0192
Tbio	Biometric hash	0.00001
Texp	Modular exponentiation in group	0.063075

Table 5 Comparative analysis based on computational cost for various stages

References	Registration phase	Login phase	Verification phase	Total Operations	Total cost
[36]	$1Th + 1Tbio + 1Tecc$	$3Th + 1Tbio + 2Tecc$	$7Th + 4Tecc$	$14Th + 2Tbio + 7Tecc$	0.14142
[27]	$1Tccm + 5Th$	$2Tccm + 1Tbio + 7Th$	$2Tccm + 6Th$	$5Tccm + 18Th$	0.1141
[39]	$1Texp + 4Th + 1Tbio$	$1Texp + 4Th + 1Tbio$	$1Texp + 4Th$	$2Texp + 12Th + 2Tbio$	0.13217
[29]	$1Tsym + 3Th$	$1Tccm + 3Tsym + 3Th$	$3Tccm + 2Tsym + 10Th$	$4Tccm + 3Tsym + 16Th$	0.11818
[58]	$2Tccm + 4Th$	$4Tccm + 7Th$	$4Tccm + 4Th$	$8Tccm + 15Th$	0.17566
[59]	$3Tccm + 2Th$	$3Tccm + 5Th$	$1Tccm + 5Th$	$7Tccm + 12Th$	0.15314
[3]	$2Tccm + 3Th$	$2Tccm + 3Th$	$2Tccm + 2Th$	$6Tccm + 8Th$	0.13012
Our	$1Tccm + 1Tbio + 4Th$	$2Tccm + 1Tbio + 5Th$	$2Tccm + 4Th$	$5Tccm + 2Tbio + 13Th$	0.11162

Table 6 Comparative analysis based on communication cost for Login and verification stage

Ref	Login phase	Verification phase	Total Operations	Total cost
[36]	$3L_h + 2L_{ecc} + L_{TS} + L_{ID}$	$3L_h + 4L_{ecc} + L_r + L_{TS}$	$6L_h + 6L_{ecc} + 2L_{TS} + L_{ID}+L_r$	2048
[27]	$7L_h + 2L_{ccm}$	$6L_h + 2L_{ccm}$	$13L_h + 4L_{ccm}$	3104
[39]	$4L_h + 1L_{exp} + 1L_{TS} + 1L_r$	$4L_h + 1L_{exp} + 1L_{TS}$	$8L_h + 2L_{exp} + 2L_{TS} + 1L_r$	1888
[29]	$3L_h + L_{ccm} + 1L_{ID}$	$10L_h + 2L_{ID} + 3L_{ccn}$	$13L_h + 4L_{ccm} + 2L_{ID}$	3168
[58]	$7L_h + 4L_{ccm} + L_{ID}$	$4L_h + 4L_{ccm}$	$11L_h + 8L_{ccm} + L_{ID}$	3840
[59]	$5L_h + 3L_{ccm}$	$5L_h + 1L_{ccm}$	$10L_h + 4L_{ccm}$	2240
[3]	$3L_h + 2L_{ccm} + L_{TS}$	$2L_h + 2L_{ccm} + L_{TS}$	$5L_h + 4L_{ccm} + 2L_{TS}$	1504
Our	$1L_h + 3L_{ccm} + L_{TS}$	$L_h + L_{ccm} + L_{TS}$	$2L_h + 4L_{ccm} + 2L_{TS}$	1408

so, a comparison of our approach with other relevant authentication systems is carried out. The numerous attacks and vulnerabilities targeted in the performance evaluation are listed in Table 3. Also, Table 3 shows that our authentication scheme can limit the vulnerabilities discussed in Sect. 5. We also comparatively discussed and analyze the other related authentication scheme.

6.1 Computation Cost: As shown in Table 5, the performance characteristics for current identical authentication schemes and our approach. Here, we compared the proposed authentication scheme with [27, 29, 36, 39, 58, 59] and [3]. Different operations, such as modular exponential (***Texp***) operations, Hash/MAC (***Th***) operations, Chebyshev chaotic map (***Tccm***), Symmetric-key encryption-decryption operation (***Tsym***), elliptic curve point multiplication operation (***Tecc***) and Biometric hash (***Tbio***) and other authentication scheme characteristics, are used to compare with our authentication scheme. The experiment result was conducted on Intel Pentium4 1 GB RAM 2600 MHz processor in [27, 60] as the cost of various operations is shown in Table 4.

Table 5 shows the comparative analysis based on the computational cost for various stages. Here, we compared with existing similar chaotic map based authentication schemes [27, 29, 36, 39, 58, 59] and [3] with our authentication scheme and found that our scheme outperforms. In comparison to the schemes mentioned, our proposed authentication scheme has a lower computing cost.

6.1 Communication Cost

Table 6 presents the comparative analysis based on communication cost between our authentication scheme and the other related existing similar chaotic map-based authentication schemes communication cost [27, 29, 36, 39, 58, 59] and [3]. In our experiment, the hash function (L_h) is 160 bits (20 bytes), the length of exponentiation operation (L_{exp}) is 256 bits (32 bytes), the output length of chebyshev chaotic map (L_{cch}) is 256 bits (32 bytes) and the output of Time-stamp (L_{TS}), random number (L_r), identity (L_{id}) is 32 bit (4 bytes). To calculate the communication cost of our proposed scheme, the two messages M1 and M2, for login and verification stage considered. The length of M1 is one time-stamp, one hash, and three chaotic map i.e. $1L_h + 3L_{ccm} + L_{TS} = 960bits$ and length of M2 is one time-stamp, one hash and one chaotic map i.e. $L_h + L_{ccm} + L_{TS} = 448bits$ therefore, the total communication cost is $2L_h + 4L_{ccm} + 2L_{TS} = 1408bits$. As shown in Table 6 it is comparatively lower in term of communication cost.

Smart cards are often constructed with limited storage capacity, and storing additional data in the smartcard reduces the device's computational performance. The suggested approach computes hash values using the chaotic hash algorithm, with a 160-bit output. The chaotic map value is 256 bits, but the random number and identity are 32 bits. The storage cost of our proposed scheme if one chaotic map and one chaotic hash i.e. ($L_h + L_{ccm}$) = 416bits.

7 Conclusion and future scope

This article proposed a provably lightweight mutually authentication and key establishment protocol using extended chaotic map for TMIS. We evaluate and compare a number of similar authentication schemes and analyze them to develop a solution that overcomes the flaws in each one. According to the security and performance analysis, the proposed method not only withstands numerous attacks but is also more efficient than other existing schemes. Our scheme is more suitable for TMIS because of its better communication and computational overhead performance.

In future, the proposed scheme can be implemented for applications on IoMT (Internet on Medical Things) and IIoT. The scheme can further be extended to offer lightweight functionality for resource constraint devices.

Funding This work is supported by SERB, Govt. of India. File No.: EEQ/2020/000053.

Data availability Data is not applicable for this work.

Declarations

Conflict of interest We declare that we have no conflict of interest.

Informed consent Informed consent was obtained from all individual participants included in the study.

References

1. Kumar D, Grover HS (2019) A secure authentication protocol for wearable devices environment using ECC. J Inf Secur Appl 47:8–15
2. Dodangeh P, Jahangir AH (2018) A biometric security scheme for wireless body area networks. J Inf Secur Appl 41:62–74
3. Dharminder D, Kumar U, Gupta P (2021) A construction of a conformal Chebyshev chaotic map based authentication protocol for healthcare telemedicine services. Complex Intell Syst. https://doi.org/10.1007/s40747-021-00441-7
4. 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):1–11
5. Qiu S, Xu G, Ahmad H, Wang L (2017) A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems. IEEE access 6:7452–7463
6. He D, Chen Y, Chen J (2012) Cryptanalysis and improvement of an extended chaotic maps-based key agreement protocol. Nonlinear Dyn 69(3):1149–1157
7. Zhao F, Gong P, Li S, Li M, Li P (2013) Cryptanalysis and improvement of a three-party key agreement protocol using enhanced Chebyshev polynomials. Nonlinear Dyn 74(1):419–427
8. 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):1–9
9. 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):1–10
10. Mullai A, Mani K (2021) Enhancing the security in RSA and elliptic curve cryptography based on addition chain using simplified Swarm Optimization and Particle Swarm Optimization for mobile devices. Int J Inf Technol 13:551–564
11. Lawal OM, Vincent OR, Agboola AAA, Folorunso O (2021) An improved hybrid scheme for e-payment security using elliptic curve cryptography. Int J Inf Technol 13:139–153
12. Lin HY (2015) Improved chaotic maps-based password-authenticated key agreement using smart cards. Commun Nonlinear Sci Numer Simul 20(2):482–488
13. Obaidat MS, Traore I, Woungang I (eds) (2019) Biometric-based physical and cybersecurity systems. Springer International Publishing, Cham
14. Yoon EJ, Jeon IS (2011) An efficient and secure Diffie-Hellman key agreement protocol based on Chebyshev chaotic map. Commun Nonlinear Sci Numer Simul 16(6):2383–2389
15. Meshram C, Lee CC, Meshram SG, Khan MK (2019) An identity-based encryption technique using subtree for fuzzy user data sharing under cloud computing environment. Soft Comput 23(24):13127–13138
16. Li CT, Lee CC, Weng CY (2014) A secure chaotic maps and smart cards based password authentication and key agreement scheme with user anonymity for telecare medicine information systems. J Med Syst 38(9):1–11
17. 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
18. Wei J, Hu X, Liu W (2012) An improved authentication scheme for telecare medicine information systems. J Med Syst 36(6):3597–3604
19. Zhu Z (2012) An efficient authentication scheme for telecare medicine information systems. J Med Syst 36(6):3833–3838
20. 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
21. Lin HY (2013) On the security of a dynamic id-based authentication scheme for telecare medical information systems. J Med Syst 37(2):1–5
22. Cao T, Zhai J (2013) Improved dynamic id-based authentication scheme for telecare medical information systems. J Med Syst 37(2):1–7
23. Guo C, Chang CC (2013) Chaotic maps-based password-authenticated key agreement using smart cards. Commun Nonlinear Sci Numer Simul 18(6):1433–1440
24. Jiang Q, Ma J, Ma Z, Li G (2013) A privacy enhanced authentication scheme for telecare medical information systems. J Med Syst 37(1):1–8
25. Yan X, Li W, Li P, Wang J, Hao X, Gong P (2013) A secure biometrics-based authentication scheme for telecare medicine information systems. J Med Syst 37(5):1–6
26. 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):1–10
27. Madhusudhan R, Nayak CS (2019) A robust authentication scheme for telecare medical information systems. Multimed Tools Appl 78(11):15255–15273
28. Radhakrishnan N, Karuppiah M (2019) An efficient and secure remote user mutual authentication scheme using smart cards for telecare medical information systems. Inf Med Unlocked 16:100092
29. Zhang L, Zhu S, Tang S (2016) Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme. IEEE J Biomed Health Inform 21(2):465–475
30. Hsieh Y-P, Lee K-C, Lee T-F, Su G-J (2022) Extended chaotic-map-based user authentication and key agreement for HIPAA privacy/security regulations. Appl Sci 12:5701. https://doi.org/10.3390/app1211570
31. Yu Z, Guangmin S, Peng Z (2022) CCMbAS: a provably secure CCM-based authentication scheme for mobile internet. Mob Inf Syst 2022:7318948. https://doi.org/10.1155/2022/7318948
32. Wu F, Xu L, Li X, Kumari S, Karuppiah M, Obaidat MS (2018) A lightweight and provably secure key agreement system for a smart grid with elliptic curve cryptography. IEEE Syst J 13(3):2830–2838
33. Sureshkumar V, Amin R, Vijaykumar VR, Sekar SR (2019) Robust secure communication protocol for smart healthcare system with FPGA implementation. Futur Gener Comput Syst 100:938–951
34. Muttoo SK, Kumar S (2012) A robust source coding watermark technique based on magnitude DFT decomposition. BIJIT, p 480
35. Srikanth GU, Geetha R, Prabhu S (2023) An efficient Key Agreement and Authentication Scheme (KAAS) with enhanced security control for IIoT systems. Int J Inf Technol. https://doi.org/10.1007/s41870-023-01173-2
36. Renuka K, Kumari S, Li X (2019) Design of a secure three-factor authentication scheme for smart healthcare. J Med Syst 43(5):1–12
37. Dharminder D, Gupta P (2021) Security analysis and application of Chebyshev chaotic map in the authentication protocols. Int J Comput Appl 43(10):1095–1103

38. Gaikwad VP, Tembhurne JV, Meshram C, Lee CC, Li CT (2021) An efficient provably secure verifier-based three-factor authentication technique using PDL for data exchange in TMIS. IEEE Access 9:108586–108600
39. Dharminder D, Mishra D, Li X (2020) Construction of RSA-based authentication scheme in authorized access to healthcare services. J Med Syst 44(1):1–9
40. Giri D, Maitra T, Amin R, Srivastava PD (2015) An efficient and robust rsa-based remote user authentication for telecare medical information systems. J Med Syst 39(1):1–9
41. 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):1–7
42. Awasthi AK, Srivastava K (2013) A biometric authentication scheme for telecare medicine information systems with nonce. J Med Syst 37(5):9964
43. Chaudhry SA, Naqvi H, Shon T, Sher M, Farash MS (2015) Cryptanalysis and improvement of an improved two factor authentication protocol for telecare medical information systems. J Med Syst 39(6):661–6611
44. Mason JC, Handscomb DC (2002) Chebyshev polynomials. CRC Press
45. Bergamo P, D'Arco P, De Santis A, Kocarev L (2005) Security of public-key cryptosystems based on Chebyshev polynomials. IEEE Trans Circuits Syst I Regul Pap 52(7):1382–1393
46. Han S, Chang E (2009) Chaotic map based key agreement with/out clock synchronization. Chaos, Solitons Fractals 39(3):1283–1289
47. Li CT, Chen CL, Lee CC, Weng CY, Chen CM (2018) A novel three-party password-based authenticated key exchange protocol with user anonymity based on chaotic maps. Soft Comput 22(8):2495–2506
48. Zhang L (2008) Cryptanalysis of the public key encryption based on multiple chaotic systems. Chaos, Solitons Fractals 37(3):669–674
49. Meshram C, Li CT, Meshram SG (2019) An efficient online/offline ID-based short signature procedure using extended chaotic maps. Soft Comput 23(3):747–753
50. Chen F, Liao X, Wong KW, Han Q, Li Y (2012) Period distribution analysis of some linear maps. Commun Nonlinear Sci Numer Simul 17(10):3848–3856
51. Meshram C, Lee CC, Meshram SG, Meshram A (2020) OOS-SSS: An efficient online/offline subtree-based short signature scheme using Chebyshev chaotic maps for wireless sensor network. IEEE Access 8:80063–80073
52. Gaikwad VP, Tembhurne JV, Meshram C, Lee CC (2021) Provably secure lightweight client authentication scheme with anonymity for TMIS using chaotic hash function. J Supercomput. https://doi.org/10.1007/s11227-020-03553-y
53. Liu W, Liu J, Wu Q, Qin B, Naccache D, Ferradi H (2018) Efficient subtree-based encryption for fuzzy-entity data sharing. Soft Comput 22(23):7961–7976
54. Meshram C, Lee CC, Ranadive AS, Li CT, Meshram SG, Tembhurne JV (2020) A subtree-based transformation model for cryptosystem using chaotic maps under cloud computing environment for fuzzy user data sharing. Int J Commun Syst 33(7):e4307
55. Xiao D, Liao X, Deng S (2005) One-way hash function construction based on the chaotic map with changeable-parameter. Chaos Solitons Fract 241:65–71
56. (2003). The AVISPA Project, Funded By the European Union in the Future and Emerging Technologies (FET Open) Programme, Project Number: IST-2001–39252. Accessed: Jul. 11, 2020. [Online]. Available: http://www.avispa-project.org/
57. SPAN (2020) A security protocol animator for AVISPA. http://www.avispa-project.org/. Accessed: Jul. 11, 2020
58. Truong TT, Tran MT, Duong AD (2020) Chebyshev polynomial-based authentication scheme in multiserver environment polynomial-based authentication scheme. Secur Commun Netw. https://doi.org/10.1155/2020/3579705
59. Zhang L, Zhu Y, Ren W, Wang Y, Xiong NN (2020) An energy efficient authentication scheme using Chebyshev chaotic map for smart grid environment. Arxiv preprint arXiv:2008.11366
60. Chaudhry SA, Naqvi H, Khan MK (2018) An enhanced lightweight anonymous biometric based authentication scheme for TMIS. Multimed Tools Appl 77(5):5503–5524
61. Burrows M, Abadi M, Needham RM (1989) A logic of authentication. Proc R Soc Lond A 426(1871):233–271
62. Mishra D, Vijayakumar P, Sureshkumar V, Amin R, Islam SH, Gope P (2018) Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks. Multimed Tools Appl 77(14):18295–18325
63. Sureshkumar V, Amin R, Anitha R (2018) A robust mutual authentication scheme for session initiation protocol with key establishment. Peer-to-Peer Netw Appl 11(5):900–916