The Journal of Supercomputing
https://doi.org/10.1007/s11227-021-04280-8

An efficient remote user authentication with key agreement procedure based on convolution-Chebyshev chaotic maps using biometric

Chandrashekhar Meshram[1] · Rabha W. Ibrahim[2] · Sarita Gajbhiye Meshram[3] · Agbotiname Lucky Imoize[4,5] · Sajjad Shaukat Jamal[6] · Sharad Kumar Barve[3]

Accepted: 21 December 2021

Abstract

The study of chaotic constructions and their associated cryptographic frameworks has sparked a lot of research interest in recent years. Latest advances in wireless technology and the proliferating limitations posed by open communication channels, biometric-enabled remote client authentication procedures with passwords have recently gained traction. In order to address this problem, this paper proposes a secure biometric-based remote user authentication procedure using convolution-Chebyshev chaotic maps with a key agreement procedure. The extended convolution-Chebyshev chaotic maps-based scheme was developed over the interval $(-\infty, +\infty)$, and the required properties for the procedure were verified rigorously. The proposed procedure provides a secure client authentication mechanism using biometrics. Additionally, the projected procedure provides a good key agreement feature with perfect forward secrecy while reducing the computation loads for smart cards. As a result, the proposed procedure outperforms related authentication procedures in terms of security and computational performance.

Keywords Mutual authentication · Convolution-Chebyshev chaotic maps · Biometric · Anonymity · Smart cards

1 Introduction

There has been a lot of research interest in analyzing chaotic systems and their possible cryptographic structures in recent years [1–3]. Specific cryptographic primitives behave in a way that is fundamentally similar to chaotic frameworks, which are described by their sensitivity to random operations and initial conditions in the

✉ Chandrashekhar Meshram
csmeshram84pdf@gmail.com

Extended author information available on the last page of the article

Published online: 12 March 2022

vicinity [4–6]. Many remote clients exchange their details with one another due to the relative ease of using the Internet, and the widespread popularity of the Internet of Things (IoT) [7]. The mechanism of remote user authentication ensures that a remote server verifies the legitimacy of a user over an insecure or open communication channel [8–10]. It is crucial to verify the identity of remote clients in this situation. In order to address this issue, Lamport [11] suggested the first authentication procedure for use in open network channels in 1981. However, it is worth mentioning that the Lamport system allows the server to keep a verification table for remote clients.

Consequently, hackers could be able to access sensitive information. The password-enabled authentication procedure is an important technique for determining the authenticity of a remote user in a client/server environment [12–15]. For instance, Sun et al. [16] posit that password-supported authentication procedures have a significant flaw because humans are not specialists at memorizing text strings. As a result, even though they know that their passwords could be insecure, most users would likely select easy-to-remember passwords.

Researchers have recently suggested several biometric-based remote client authentication procedures [17–20]. The work in [17] in particular presented an improved biometric-based authentication procedure for telecare medicine information systems (TMIS) based on an elliptic curve cryptosystem. By comparison, the work in [18] projected an improved and robust biometrics-based three-factor authentication procedure for applications in multi-server environments. In a similar fashion to work in [18], a robust biometrics-based authentication procedure for a multi-server setting has been presented [19]. Due to Odelu et al. [20], the work presented a secure biometrics-based multi-server authentication procedure using smart cards. Essentially, the biometric system, based on pattern recognition, collects biometric data from an individual. The system accomplishes this by extracting and comparing a feature set from the information to a database template set [21–24]. According to Das [25], biometric keys have several advantages listed as follows. Biometric keys cannot be lost or forgotten. They are complicated to share or copy. They are also tough to distribute or forge, not easy to break, and cannot be guessed easily.

Additionally, biometric-supported remote client authentication procedures are highly efficient and safer than predictable password-based remote client authentication procedures. In 2014, Chuang et al. [26] introduced a trust computing-based anonymous multi-server authentication with key agreement procedure, leveraging smart-cards and biometrics. According to Chuang et al. [26], the procedure is quite simple to use and allows for multi-server authentication and user anonymity. Later, in 2014 and 2015, Mishra et al. [27] and Lin et al. [28] examined Chuang et al. [26] procedure and found several flaws. In order to address these issues, they suggested a stable anonymous three-factor authentication procedure with superior capabilities. In 2015, Lu et al. [29] demonstrated that Mishra et al.'s [27] approach is highly vulnerable to replay attacks and includes an insecure password altering process. For multi-server architecture, they suggested a robust biometric-based authentication procedure.

In 2015, Mir et al. [30] projected an authentication procedure using Elliptic Curve Cryptography (ECC) for telemedicine networks. Also, Chaudhry et al. [31] demonstrated that Mir et al.'s procedure [30] is vulnerable to a misplaced smart card attack and fails to provide the required user anonymity. In 2016, Zhu [32] proposed a multi-server procedure for privacy security focused on chaotic map operations. However, their procedure is limited due to their vulnerability to a privileged insider attack. This is because an RC system insider operating as an attacker can guess a client's password using stored information on the client's device and registration appeal information throughout the registration process.

In 2018, Qi et al. [33] showed that Chaudhry et al.'s [31] procedure could not achieve the perfect forward secrecy and failed a denial-of-service attack. Qi et al. [33] proposed a new procedure to address the limitations inherent in Chaudhry et al.'s procedure [31]. It is worthy of note that the scheme due to Qi et al. [33] can withstand various attacks. Recently, Sahoo et al. [34] presented remarkable results that show the limitations of Qi et al.'s procedure. Sahoo et al. [34] noted that Qi et al.'s procedure [33] could not protect against the key compromise impersonation attack, known session-specific temporary information attack, and offline password guessing attack. In order to address these issues, Sahoo et al. [34] advised an enhanced new procedure based on ECC and demonstrating the strengths to resist various attacks. A summary of some related works is given in Table 1.

The preceding works of literature demonstrate that current biometric-empowered remote client authentication with key agreement procedures has varying security strengths and lower computational overheads. However, when exposed to several high-level adversarial attacks, most of the existing schemes show limited existential unforgeability.

Additionally, remote user authentication using biometric applications with key agreement procedures is critical to the design of future security systems. However, the idea of employing convolution-Chebyshev chaotic maps for biometric-based remote user authentication has not been addressed adequately. Addressing this problem is critical to overcoming the vast limitations of current remote user authentication using biometric with key agreement procedures.

Also, modern cryptography focused on chaos theory, such as signature techniques [35–38], authentication [9, 39, 40], information hiding techniques [41–43], encryption techniques for cloud computing environments [44–48], mobile healthcare [49], secure and adaptive intelligent learning [50–53], and hash functions [54], which has received a lot of attention in recent years. Thus, the idea of using cryptographic-based chaotic maps to create a robust authentication scheme is not out of place.

Based on chaos theory, the projected procedure will allow a client to communicate with a server anonymously while providing mutual authentication among the client and the server. Thus, the current paper introduces an efficient convolution-Chebyshev chaotic maps-based remote client authentication with key agreement procedure using biometric to address the shortcomings of the related procedures in the literature.

1.1 Contributions

The following are the main contributions of this paper:

Table 1 Related works

References	Key contributions	Limitations
Chuang et al. [26]	The work projected a trust computing-based anonymous multi-server authentication with key agreement procedure, leveraging smartcards and biometrics	The scheme requires a stable anonymous three-factor authentication procedure with superior capabilities. In addition, the scheme shows limited security against multiple attacks; replay, smart card loss and offline password guessing
Mishra et al. [27]	The study described a smart card-based secure user anonymity-preserving biometric-based multi-server authenticated key agreement procedure	The procedure is highly vulnerable to replay attacks and includes an insecure password altering process
Lu et al. [29]	The procedure presents the limitations of the procedure highlighted by Mishra et al. [27], and suggested a robust biometric-based authentication procedure for multi-server architecture	Practical deployment of the technique is not elaborated, and a possible extension of the scheme is not highlighted
Mir et al. [30]	The work projected an authentication procedure using Elliptic Curve Cryptography (ECC) for telemedicine networks	The procedure is vulnerable to a misplaced smart card attack and fails to provide the required user anonymity
Chaudhry et al. [31]	In this work, an improved lightweight anonymous biometric based authentication procedure for telemedicine information system (TMIS) was presented	The procedure could not achieve the perfect forward secrecy and failed a denial-of-service attack
Zhu [32]	Zhu [32] proposed a multi-server procedure for privacy security focused on chaotic map operations	The procedure is vulnerable to a privileged insider attack
Qi et al. [33]	The work presented a new biometrics-based mutual authentication procedure with key agreement based on elliptic curve cryptography to address the limitations inherent in Chaudhry et al.'s procedure [31]	The procedure could not protect against the key compromise impersonation attack, known session-specific temporary information attack, and offline password guessing attack
Sahoo et al. [34]	The work presented remarkable results that show the limitations of Qi et al.'s procedure [33]. Specifically, an improved procedure based on ECC was projected. The security of the scheme was demonstrated using several attacks	The procedure shows high computational complexity and high communication cost. Also, there is a need to establish a security model for chaotic-based authentication and key agreement procedure

We projected an effective remote user authentication using biometric with a key agreement procedure, leveraging convolution-Chebyshev chaotic maps.

We demonstrated that the proposed remote user authentication using biometric with key agreement procedure has the lowest storage expense in contrast to other procedures in the literature.

We showed that our projected scheme gives high-level security. The key innovation in our proposed work is that while maintaining high performance, the proposed remote user authentication using biometric with key agreement procedure provides high-level security.

We demonstrate that the proposed remote user authentication using biometric with key agreement procedure can be easily implemented in various low-power and low-processing-power devices.

1.2 Roadmap

The remainder of this article is planned as follows. In Sect. 2, we introduce the definitions of Chebyshev chaotic maps and their extension. In Sect. 3, we developed the new version of chaotic maps and discussed their properties. Then, the projected procedure is presented in Sect. 4. In Sect. 5, we review the projected procedure and prove that it can withstand various sophisticated attacks. In Sect. 6, we examined the performance of the presented procedure. Finally, Sect. 7 concludes the paper and discusses future prospects.

2 Preliminaries

The Chebyshev polynomial and extended chaotic maps are discussed in this section. The symbolizations used in our projected procedure are presented in Table 2.

2.1 Chebyshev chaotic maps

This section looks at Chebyshev polynomials (CP) [55] and examines their functionalities, as shown in Fig. 1. The CP $\mathrm{T}_r(\chi)$ is a polynomial with degree n in the variant of χ. Let n be an integer, and $\chi \in [-1, 1]$ be the version. The CP is defined as follows:

$$\begin{aligned}
&\mathrm{T_n}(\chi) = \cos\left(\mathrm{n} \times \cos^{-1}(\chi)\right),\\
&\mathrm{T_0}(\chi) = 1\\
&\mathrm{T_1}(\chi) = \chi\\
&\mathrm{T_n}(\chi) = 2\chi\mathrm{T_{n-1}}(\chi) - \mathrm{T_{n-2}}(\chi);\ \mathrm{n} \geq 2
\end{aligned}$$

where $\cos^{-1}$ and $\cos(x)$ are trigonometric functions [56] considered as $\cos^{-1} : [-1, 1] \rightarrow [0, \pi]$ and $\cos : \mathrm{R} \rightarrow [-1, 1]$. Figure 1 shows a few examples of CPs for $n = 1, 2, 3, 4, 5$.

Table 2 Symbolizations used in the presented procedure

Symbolization	Meaning
$\mathcal{U}_i$	User
$\mathcal{RC}_i$	Reliable registration center
$\mathcal{S}_i$	Server
pwd_i	Password shared among $\mathcal{U}_i$ and $\mathcal{S}_i$
id_i	$\mathcal{U}_i$ user's identity
B_i	$\mathcal{U}_i$ user's biometric template
q_1	A large prime number
$\mathtt{b}$	The registration center chooses a random integer
w	The registration center chooses a random number
$p\mathtt{k}$	$\mathcal{RC}_i' s$ public key, where $p\mathtt{k} \equiv T_b(w)\left(\mathrm{mod}\, q_1\right)$
$\mathtt{u}, \mathtt{v}$	Random integers
τ_i	The time-stamp
$\mathcal{H}(\cdot)$	A safe one-way hash function
$\|$	The concatenation operation
$\mathtt{T}$	Chebyshev chaotic operation
$\boldsymbol{T}$	Convolution-Chebyshev chaotic map
$\oplus$	The exclusive-or operation

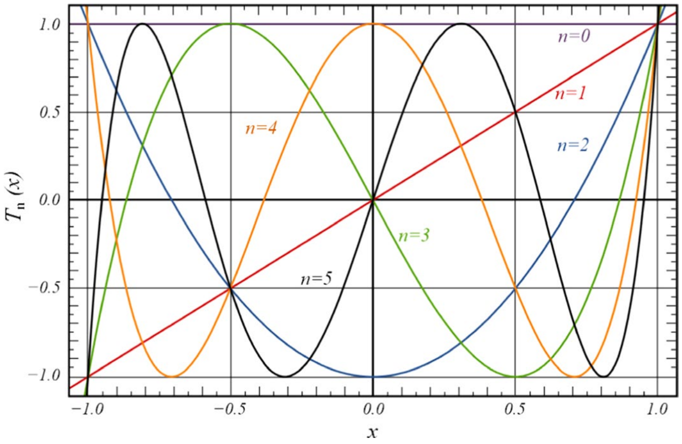

Fig. 1 Chebyshev polynomials

2.2 Properties of Chebyshev polynomials

Two significant properties characterize Chebyshev polynomials [38, 45, 49, 57]. These are the chaotic and semi-group properties.

(a) The chaotic property:

The Chebyshev polynomial map defined as $\mathrm{T}_r : [-1,1] \rightarrow [-1,1]$ with degree $n > 1$, is a chaotic map having its invariant density function given as $f^*(\chi) = \frac{1}{\left(\pi\sqrt{1-\chi^2}\right)}$ for some positive Lyapunov exponent $\lambda = \text{In}\, n > 0$.

(b) The semi-group property:

$$\begin{aligned} \mathrm{T}_{\mathrm{w}}\left(\mathrm{T}_{\mathrm{l}}(\chi)\right) &= \cos\left(\mathrm{w}\cos^{-1}\left(\cos\left(\mathrm{l}\cos^{-1}(\chi)\right)\right)\right) \\ &= \cos\left(\mathrm{wl}\cos^{-1}(\chi)\right) \\ &= \mathrm{T}_{\mathrm{lw}}(\chi) \\ &= \mathrm{T}_{\mathrm{l}}\left(\mathrm{T}_{\mathrm{w}}(\chi)\right), \end{aligned}$$

where l and w are positive integers and $\chi \in [-1,1]$.

2.3 Computational problems

Two challenges that are known to be quite hard to handle within polynomial time are observed in Chebyshev polynomials [35, 36, 38, 39, 45]. These are defined as follows:

(1) Given two exponents χ and Y, the task of the discrete Log (DL) is to estimate the integer w with the end goal $\mathrm{T}_{\mathrm{w}}(\chi) = \mathrm{Y}$.
(2) Given three exponents χ, $\mathrm{T}_{\mathrm{w}}(\chi)$, and $\mathrm{T}_{\ell}(\chi)$, the task of the Diffie–Hellman problem (DHP) is to estimate the exponent $\mathrm{T}_{\mathrm{w}\ell}(\chi)$.

2.4 Extended chaotic maps

It was established by Zhang [58] that the above semigroup property holds for CPs within the interval $(-\infty, +\infty)$. This can be strengthened by:

$$\mathrm{T}_{\mathrm{n}}(\chi) = \left(2\chi\mathrm{T}_{\mathrm{n-1}}(\chi) - \mathrm{T}_{\mathrm{n-2}}(\chi)\right)\left(\bmod q_1\right)$$

where $\chi \in (-\infty, +\infty)$, $\mathrm{n} \geq 2$ and q_1 is a large prime. Now, we reflect on the recurrence relations $\mathrm{T}_{\mathrm{n}}(\chi) = \left(12\mathrm{T}_{\mathrm{n-1}}(\chi) - \mathrm{T}_{\mathrm{n-2}}(\chi)\right)(\bmod 13)$ with $\mathrm{T}_0(\chi) = 1$ and $\mathrm{T}_1(\chi) = 6$, where $q_1 = 13$. Then, $\mathrm{T}_{\mathrm{n}}(\chi)$ created by this recurrence is 1, 6, 6, 1, 6, 6, …… with T=3 period [45, 59]. Obviously,

$\mathrm{T}_{\mathrm{w}}\left(\mathrm{T}_{\mathrm{l}}(\chi)\right) \equiv \mathrm{T}_{\mathrm{lw}}(\chi) \equiv \mathrm{T}_{\mathrm{l}}\left(\mathrm{T}_{\mathrm{w}}(\chi)\right)\left(\bmod q_1\right)$,

As a result, the semigroup assets holds and the improved Chebyshev polynomials commute as well.

3 Main results for convolution-Chebyshev chaotic maps

In this section, we briefly familiarize the convolution-Chebyshev summation (CCS). Also, we developed a new version of Chebyshev chaotic maps, known as convolution-Chebyshev chaotic maps (CCCM).

3.1 Convolution-Chebyshev summation (CCS)

Convolution-Chebyshev summation (CCS) is a formula of several variations of any summation method for summing possibly divergent formal power series, introduced by Chebyshev summation.

3.1.1 Convolution-Chebyshev chaotic maps

Definition 1 For two power series in z, the convolution product (Hadamard product) is defined as follows [60]:

$$\phi(\varsigma) * \psi(\varsigma) = \sum_{n=0}^{\infty} \phi_n \psi_n \varsigma^n,$$

where $\phi(\varsigma) = \sum_{n=0}^{\infty} \phi_n \varsigma^n$ and $\psi(\varsigma) = \sum_{n=0}^{\infty} \psi_n \varsigma^n$.

We define a transform called convolution-Chebyshev summation (CCS) by using the convolution product and the summation formula of Chebyshev polynomials.

$$\mathbb{T}_{\chi}(\varsigma) := \sum_{n=0}^{\infty} \mathrm{T}_n(\chi)\varsigma^n = \frac{1 - \varsigma\chi}{1 - 2\varsigma\chi + \varsigma^2}.$$

Note that

$$\mathrm{T}_n(\chi) = n \sum_{k=0}^{n} (-2)^k \frac{(n+k-1)!}{(n-k)!(2k)!}(1-\chi)^k, \quad n > 0,$$

where

$$\begin{aligned} &\mathrm{T}_0(\chi) = 1 \\ &\mathrm{T}_1(\chi) = \chi \\ &\mathrm{T}_{n+1}(\chi) = 2\chi\,\mathrm{T}_n(\chi) - \mathrm{T}_{n-1}(\chi). \end{aligned}$$

as follows:

Definition 2 Define a power series in ς

$$\phi(\varsigma) = \sum_{n=0}^{\infty} \phi_n \varsigma^n.$$

Define the transform $\mathcal{T}_{\chi}$ of ϕ by

$$\mathbf{T}_{\chi}(\varsigma) := \mathbb{T}_{\chi}(\varsigma) * \phi(\varsigma) \equiv \sum_{n=0}^{\infty} \phi_n T_n(\chi)\varsigma^n.$$

Note that

$$\mathbf{T}^k_\chi(\varsigma) = \mathbf{T}_\chi(\varsigma) *, \underbrace{\ldots}_{k\text{-times}}, * \mathbf{T}_\chi(\varsigma)$$

and for all χ, The CCS $\mathbf{T}_\chi(\varsigma)$ satisfies the recurrent convolution

$$\mathbf{T}_\chi(\varsigma) = \sum_{n=0}^{\infty} \phi_n \left[2\chi\, \mathtt{T}_{n-1}(\chi) - \mathtt{T}_{n-2}(\chi)\right] \varsigma^n.$$

Finally, the dynamic plot of the suggested CCS is shown in Fig. 2.

3.1.2 Extended chaotic maps by using convolution product

Zhang [58] established that the above semigroup properties hold for Chebyshev polynomials defined on the $(-\infty, +\infty)$ interval, which can improve the assets, as follows (see Sect. 2):

$$\mathtt{T}_{\mathrm{n}}(\chi) = \left(2\chi \mathtt{T}_{\mathrm{n-1}}(\chi) - \mathtt{T}_{\mathrm{n-2}}(\chi)\right)\left(\operatorname{mod} q_1\right)$$

Obviously, $\mathtt{T}_n\left(\mathtt{T}_l(\chi)\right) \equiv \mathtt{T}_{nl}(\chi) \equiv \mathtt{T}_l\left(\mathtt{T}_n(\chi)\right)$ (mod q_1) , so the semigroup possessions hold and the enhanced Chebyshev polynomials commute under composition.

Using the convolution approach for all $\chi \in (-\infty, +\infty)$, we get the following result:

Theorem 3.1 *Consider the power series $\phi(\varsigma) = \sum_{n=0}^{\infty} \phi_n \varsigma^n$. The recurrent and semigroup relations for all $\chi \in (-\infty, +\infty)$ are given by*

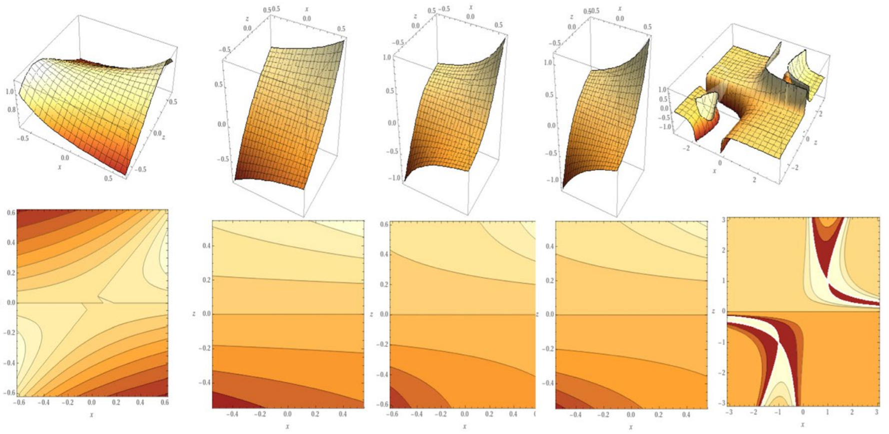

Fig. 2 Three-dimensional plot and the contour plot for the functions $\mathbb{T}_\chi(z), \phi(\varsigma) = \frac{\varsigma}{(1-x\varsigma)}, \mathbb{T}_\chi(\varsigma) * \phi_\chi(\varsigma)$ of first order and $\phi_\chi(\varsigma) = \frac{\varsigma}{(1-x\varsigma)^2}$ and $\mathbb{T}_\chi(\varsigma), \phi_\chi(\varsigma)$ for the second order, respectively

(1)
$$\left(\mathbf{T}_{\chi}^{m}(\varsigma)\right) = \mathbf{T}_{\chi}^{m-1}\left(\boldsymbol{T}_{\chi}(\varsigma)\right) = \boldsymbol{T}_{\chi}^{m-2}\left(\boldsymbol{T}_{\chi}^{2}(\varsigma)\right)$$

(2)
$$\mathbf{T}_{\chi}^{k}\left(\mathbf{T}_{\chi}^{m}(\varsigma)\right) = \mathbf{T}_{\chi}^{km}(\varsigma).$$

Proof For the first part, it is easy to verify the result directly from the convolution product. For the second part, we use the definition of the generalized formula, we get

$$\begin{aligned}
\mathbf{T}_{\chi}^{k}\left(\mathbf{T}_{\chi}^{m}(\varsigma)\right) &= \mathbf{T}_{\chi}\left(\mathbf{T}_{\chi}^{m}(\varsigma)\right) *, \underbrace{\ldots}_{k\text{-times}}, * \,\mathbf{T}_{\chi}\left(\mathbf{T}_{\chi}^{m}(\varsigma)\right) \\
&= \mathbf{T}_{\chi}\left(\mathbf{T}_{\chi}(\varsigma) *, \underbrace{\ldots}_{m\text{-times}}, * \,\mathbf{T}_{\chi}(\varsigma)\right) *, \underbrace{\ldots}_{k\text{-times}\mathbf{T}_{\chi}(\varsigma)}, * \,\mathbf{T}_{\chi}\left(\mathbf{T}_{\chi}(\varsigma) *, \underbrace{\ldots}_{m\text{-times}}, * \,\mathbf{T}_{\chi}(\varsigma)\right) \\
&= \mathbf{T}_{\chi}(\varsigma) *, \underbrace{\ldots}_{km\text{-times}}, * \,\mathbf{T}_{\chi}(\varsigma) \\
&= \mathbf{T}_{\chi}^{km}(\varsigma).
\end{aligned}$$

4 The proposed procedure

In this section, the proposed scheme using the convolution-Chebyshev chaotic maps is presented. The flowchart of authentication using biometric is shown in Fig. 3. The registration center $\mathcal{RC}_i$ starts by picking a random number w and an arbitrary integer b, then computing $p\mathrm{k} \equiv \boldsymbol{T}_b(w)\left(\bmod q_1\right)$. The master secret key b is held secretly by the registration center $\mathcal{RC}_i$. The registration, authentication, login, and password change stages are all part of our presented scheme. The detailed steps of these stages will now be outlined in the subsections as follows.

4.1 Registration stage

The remote $\mathcal{U}_i$ user must follow the steps below to register and become new authorized users in the framework, as shown in Fig. 4.

(1) The user enters their password pwd_i, identity id_i, a n arbitrary number, and her/his personal biometric $\boldsymbol{B}_i$ on a specific computer, then estimates $\psi_i = \mathcal{H}\left(\boldsymbol{B}_i\right)$. $\mathcal{U}_i$ then sends $\{id_i, \psi_i = \mathcal{H}\left(\boldsymbol{B}_i\right), \mathcal{H}\left(pwd_i \parallel \boldsymbol{B}_i \parallel \mathrm{n}\right)\}$ via a protected channel to the $\mathcal{RC}_i$ registration center.

(2) The registration center calculates the succeeding $\mathcal{RC}_i$:

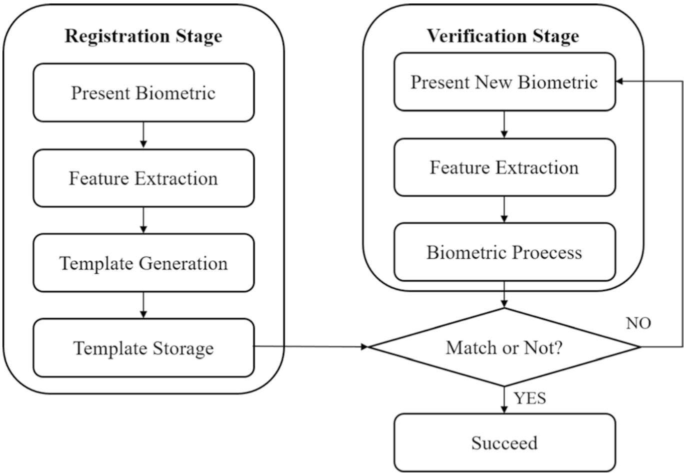

Fig. 3 Flowchart of authentication using biometric

$$\Omega_i = \mathcal{H}(id_i \parallel b),$$
$$\mathcal{W}_i = \mathcal{H}(pwd_i \parallel \boldsymbol{B}_i \parallel \mathrm{n}) \oplus \psi_i,$$
$$\mathcal{Y}_i = \Omega_i \oplus \mathcal{W}_i.$$

$\mathcal{RC}_i$ embeds $(id_i, \mathcal{H}(.), \mathcal{Y}_i, w, p\mathrm{k}, q_1)$ in the user's smart card (SC) and sends it over a protected channel to the user $\mathcal{U}_i$.

(3) $\mathcal{U}_i$ calculates $\boldsymbol{B}pwd = \boldsymbol{B}_i \oplus \mathcal{H}(pwd_i)$ after obtaining the smart card and inserting n and $\boldsymbol{B}pwd$ into the SC to complete the registration.

4.2 Login stage

When a legal user $\mathcal{U}_i$ wishes to access the server $\mathcal{S}_i$ in this process, as shown in Fig. 5, they must do the following:

(1) $\mathcal{U}_i$ inserts their SC into the card reader and select a specific device for their biometric template $\boldsymbol{B}_i$ and password pwd_i.

(2) The values $\boldsymbol{B}_i' = \boldsymbol{B}pwd \oplus \mathcal{H}(pwd_i)$ is computed and $\boldsymbol{B}_i = \boldsymbol{B}_i'$ is checked by the SC. The smart card would refuse the request if $\boldsymbol{B}_i \neq \boldsymbol{B}_i'$.

(3) The SC creates a u and calculates

$$\psi_i = \mathcal{H}(\boldsymbol{B}_i),$$
$$\mathcal{W}_i' = \mathcal{H}(pwd_i \parallel \boldsymbol{B}_i \parallel \mathrm{n}) \oplus \psi_i$$
$$\Omega_i' = \mathcal{Y}_i \oplus \mathcal{W}_i',$$
$$\mathfrak{W}_1 \equiv \boldsymbol{T}_{\mathrm{u}}(w)(\bmod q_1),$$
$$\mathfrak{W}_2 \equiv \boldsymbol{T}_{\mathrm{u}}(p\mathrm{k})(\bmod q_1),$$
$$\mathrm{n}id_i = id_i \oplus \mathcal{H}(\mathfrak{W}_1 \parallel \mathfrak{W}_2)$$
$$\gamma = \mathcal{H}(id_i \parallel \mathrm{n}id_i \parallel \Omega_i' \parallel \mathfrak{W}_1 \parallel \mathfrak{W}_2 \parallel \tau_1).$$

	$\boldsymbol{\mathcal{RC}_i}$
Creates a random number n	

$$\xrightarrow{\boldsymbol{id_i},\ \boldsymbol{\psi_i} = \boldsymbol{\mathcal{H}}(\boldsymbol{B_i}),\ \boldsymbol{\mathcal{H}}(\boldsymbol{pwd_i} \parallel \boldsymbol{B_i} \parallel \mathrm{n})}$$

$\boldsymbol{\Omega_i} = \boldsymbol{\mathcal{H}}(\boldsymbol{id_i} \parallel \mathrm{b})$

$\boldsymbol{\mathcal{W}_i} = \boldsymbol{\mathcal{H}}(\boldsymbol{pwd_i} \parallel \boldsymbol{B_i} \parallel \mathrm{n}) \oplus \boldsymbol{\psi_i}$

$\boldsymbol{Y_i} = \boldsymbol{\Omega_i} \oplus \boldsymbol{\mathcal{W}_i}$

$$\xleftarrow{\text{Smart card } (\boldsymbol{id_i}, \boldsymbol{\mathcal{H}}(.), \boldsymbol{Y_i}, \boldsymbol{w}, \boldsymbol{p}\mathrm{k}, \boldsymbol{q_1})}$$

Inserts n and $\boldsymbol{Bpwd} = \boldsymbol{B_i} \oplus \boldsymbol{\mathcal{H}}(\boldsymbol{pwd_i})$

Fig. 4 Registration stage of the projected procedure

$\boldsymbol{\mathcal{U}_i}$	$\boldsymbol{\mathcal{S}_i}$
Inserts the smart card and inputs $\boldsymbol{pwd_i}$, $\boldsymbol{B_i}$	
$\boldsymbol{B_i}' = \boldsymbol{Bpwd} \oplus \boldsymbol{\mathcal{H}}(\boldsymbol{pwd_i})$	
Verifies $\boldsymbol{B_i}? = \boldsymbol{B_i}'$	
Generates $\boldsymbol{u}$	
$\boldsymbol{\psi_i} = \boldsymbol{\mathcal{H}}(\boldsymbol{B_i})$	
$\boldsymbol{\mathcal{W}_i}' = \boldsymbol{\mathcal{H}}(\boldsymbol{pwd_i} \parallel \boldsymbol{B_i} \parallel \mathrm{n}) \oplus \boldsymbol{\psi_i}$	
$\boldsymbol{\Omega_i}' = \boldsymbol{Y_i} \oplus \boldsymbol{\mathcal{W}_i}'$	
$\mathfrak{W}_1 \equiv \boldsymbol{T}_{\mathrm{u}}(\boldsymbol{w}) \ (\mathbf{mod}\ \boldsymbol{q_1})$	
$\mathfrak{W}_2 \equiv \boldsymbol{T}_{\mathrm{u}}(\boldsymbol{p}\mathrm{k}) \ (\mathbf{mod}\ \boldsymbol{q_1})$	
$\mathrm{n}\boldsymbol{id_i} = \boldsymbol{id_i} \oplus \boldsymbol{\mathcal{H}}(\mathfrak{W}_1 \parallel \mathfrak{W}_2)$	
$\boldsymbol{\Upsilon} = \boldsymbol{\mathcal{H}}(\boldsymbol{id_i} \parallel \mathrm{n}\boldsymbol{id_i} \parallel \boldsymbol{\Omega_i}' \parallel \mathfrak{W}_1 \parallel \mathfrak{W}_2 \parallel \boldsymbol{\tau_1})$	

$$\xrightarrow{\mathrm{n}\boldsymbol{id_i},\ \mathfrak{W}_1,\ \boldsymbol{\Upsilon},\ \boldsymbol{\tau_1}}$$

Fig. 5 Login stage of the projected procedure

(4) The user $\mathcal{U}_i$ sends $\{\mathrm{n}id_i, \mathfrak{W}_1, \gamma, \tau_1\}$ to $\mathcal{S}_i$.

4.3 Authentication stage

The server $\mathcal{S}_i$ carries out the following phases to access mutual authentication after receiving the login appeal messages, as shown in Fig. 6.

(1) Upon receiving $\{\mathrm{n}id_i, \mathfrak{W}_1, \gamma, \tau_1\}$, $\mathcal{S}_i$ tests the legitimacy of τ_1 by the examination, if the equation $\tau' - \tau_1 > \Delta\tau$ holds, where τ' is the time when the server obtains

$\boldsymbol{\mathcal{U}_i}$		$\boldsymbol{\mathcal{S}_i}$
		Checks $\boldsymbol{\tau}' - \boldsymbol{\tau_1} > \Delta\boldsymbol{\tau}$
		$\mathfrak{W}_2' \equiv \boldsymbol{T}_{\mathrm{b}}(\mathfrak{W}_1)$ **(mod** $\boldsymbol{q_1}$**)**
		$\boldsymbol{id_i}' = \mathrm{n}\boldsymbol{id_i} \oplus \boldsymbol{\mathcal{H}}(\mathfrak{W}_1 \parallel \mathfrak{W}_2')$
		Checks $\boldsymbol{id_i}'$
		$\boldsymbol{\Omega_i}'' = \boldsymbol{\mathcal{H}}(\boldsymbol{id_i}' \parallel \mathrm{b})$
		$\boldsymbol{\Upsilon}' = \boldsymbol{\mathcal{H}}(\boldsymbol{id_i}' \parallel \mathrm{n}\boldsymbol{id_i} \parallel \boldsymbol{\Omega_i}'' \parallel \mathfrak{W}_1 \parallel \mathfrak{W}_2' \parallel \boldsymbol{\tau_1})$
		Verifies $\boldsymbol{\Upsilon}'? = \boldsymbol{\Upsilon}$
		Generates v
		$\mathfrak{m}_3 \equiv \boldsymbol{T}_{\mathrm{v}}(\boldsymbol{w})$ **(mod** $\boldsymbol{q_1}$**)**
		$\boldsymbol{\mu} = \boldsymbol{\mathcal{H}}(\boldsymbol{id_i}' \parallel \boldsymbol{\Omega_i}'' \parallel \mathfrak{W}_2' \parallel \mathfrak{W}_3 \parallel \boldsymbol{\tau_2})$
	$\mathfrak{m}_3,\ \boldsymbol{\mu},\ \boldsymbol{\tau_2}$ $\longleftarrow$	
Checks $\boldsymbol{\tau}' - \boldsymbol{\tau_2} > \Delta\boldsymbol{\tau}$		
$\boldsymbol{\mu}' = \boldsymbol{\mathcal{H}}(\boldsymbol{id_i} \parallel \boldsymbol{\Omega_i}' \parallel \mathfrak{W}_2 \parallel \mathfrak{W}_3 \parallel \boldsymbol{\tau_2})$		
Verifies $\boldsymbol{\mu}'? = \boldsymbol{\mu}$		
$\mathfrak{W}_4 \equiv \boldsymbol{T}_{\mathrm{u}}(\mathfrak{W}_3) \equiv \boldsymbol{T}_{\mathrm{uv}}(\boldsymbol{w})$ **(mod** $\boldsymbol{q_1}$**)**		
$\boldsymbol{\xi} = \boldsymbol{\mathcal{H}}(\boldsymbol{id_i} \parallel \boldsymbol{\Omega_i}' \parallel \mathfrak{W}_2 \parallel \mathfrak{W}_4 \parallel \boldsymbol{\tau_3})$		
	$\boldsymbol{\xi},\ \boldsymbol{\tau_3}$ $\longrightarrow$	
		Checks $\boldsymbol{\tau}' - \boldsymbol{\tau_3} > \Delta\boldsymbol{\tau}$
		$\mathfrak{W}_4' \equiv \boldsymbol{T}_{\mathrm{v}}(\mathfrak{W}_1) \equiv \boldsymbol{T}_{\mathrm{uv}}(\boldsymbol{w})$ **(mod** $\boldsymbol{q_1}$**)**
		$\boldsymbol{\xi}' = \boldsymbol{\mathcal{H}}(\boldsymbol{id_i}' \parallel \boldsymbol{\Omega_i}'' \parallel \mathfrak{W}_2' \parallel \mathfrak{W}_4' \parallel \boldsymbol{\tau_3})$
		Verifies $\boldsymbol{\xi}'? = \boldsymbol{\xi}$

Fig. 6 Authentication stage of the presented procedure

the messages from $\mathcal{U}_i$ and $\Delta\tau$ represents the predetermined permissible time period of transmission delay. $\mathcal{S}_i$ rejects $\mathcal{U}_i$ if the equation holds.

(2) $\mathcal{S}_i$ calculates $\mathfrak{W}_2' \equiv \boldsymbol{T}_b(\mathfrak{W}_1)(\mathrm{mod}\, q_1)$, $id_i' = \mathrm{n}id_i \oplus \mathcal{H}(\mathfrak{W}_1 \parallel \mathfrak{W}_2')$ and checks the legitimacy of id_i'.

(3) $\mathcal{S}_i$ calculates $\Omega_i'' = \mathcal{H}(id_i' \parallel b)$ and $\gamma' = \mathcal{H}(id_i' \parallel \mathrm{n}id_i \parallel \Omega_i'' \parallel \mathfrak{W}_1 \parallel \mathfrak{W}_2' \parallel \tau_1)$.

(4) Then, $\mathcal{S}_i$ verifies whether γ' equals to γ. If $\gamma' \neq \gamma$, $\mathcal{S}_i$ stops the session.

(5) If $\gamma' = \gamma$, $\mathcal{S}_i$ arbitrarily selects an integer v and calculates $\mathfrak{W}_3 \equiv \boldsymbol{T}_{\mathrm{v}}(w)(\mathrm{mod}\, q_1)$ and $\mu = \mathcal{H}(id_i' \parallel \Omega_i'' \parallel \mathfrak{W}_2' \parallel \mathfrak{W}_3 \parallel \tau_2)$. Then, $\mathcal{S}_i$ sends $\{\mathfrak{W}_3, \mu, \tau_2\}$ to $\mathcal{U}_i$.

(6) $\mathcal{U}_i$ tests the validity of τ_2 by testing, if the equation $\tau' - \tau_2 > \Delta\tau$ holds after obtaining $\{\mathfrak{W}_3, \mu, \tau_2\}$. $\mathcal{U}_i$ rejects $\mathcal{S}_i$ if the equation holds.

(7) $\mathcal{U}_i$ checks whether $\mu'? = \mu$ by computing $\mu' = \mathcal{H}(id_i \parallel \Omega_i' \parallel \mathfrak{W}_2 \parallel \mathfrak{W}_3 \parallel \tau_2)$. $\mathcal{U}_i$ will terminate the session if they are not equal. Otherwise, $\mathcal{U}_i$ computes $\mathfrak{W}_4 \equiv \boldsymbol{T}_{\mathrm{u}}(\mathfrak{W}_3) \equiv \boldsymbol{T}_{\mathrm{uv}}(w)(\mathrm{mod}\, q_1)$ and $\xi = \mathcal{H}(id_i \parallel \Omega_i' \parallel \mathfrak{W}_2 \parallel \mathfrak{W}_4 \parallel \tau_3)$. Then, $\mathcal{U}_i$ sends $\{\xi, \tau_3\}$ to $\mathcal{S}_i$.

(8) $\mathcal{S}_i$ tests the validity of τ_3 by testing, if the equation $\tau' - \tau_3 > \Delta\tau$ holds as it receives $\{\xi, \tau_3\}$. $\mathcal{S}_i$ rejects $\mathcal{U}_i$ if the equation holds. Otherwise, $\mathcal{S}_i$ computes $\mathfrak{W}_4' \equiv \boldsymbol{T}_{\mathrm{v}}\left(\mathfrak{W}_1\right) \equiv \boldsymbol{T}_{\mathrm{uv}}(w)\left(\operatorname{mod} q_1\right)$ and $\xi' = \mathcal{H}\left(id_i' \parallel \Omega_i'' \parallel \mathfrak{W}_2' \parallel \mathfrak{W}_4' \parallel \tau_3\right)$ and tests if $\xi'? = \xi$.

(9) $\mathcal{S}_i$ approves $\mathcal{U}_i$'s login appeal if it holds, and the verification is complete. Then, using a symmetric cryptosystem, both $\mathcal{U}_i$ and $\mathcal{S}_i$ will connect with each other using the session key $\mathfrak{W}_4$ and $\mathfrak{W}_4'$.

Subsequently $p\mathrm{k} \equiv \boldsymbol{T}_b(w)\left(\operatorname{mod} q_1\right)$, $\mathfrak{W}_1 \equiv \boldsymbol{T}_{\mathrm{u}}(w)\left(\operatorname{mod} q_1\right)$, $\mathfrak{W}_2 \equiv \boldsymbol{T}_{\mathrm{u}}(p\mathrm{k})\left(\operatorname{mod} q_1\right)$, and $\mathfrak{W}_3 \equiv \boldsymbol{T}_{\mathrm{v}}(w)\left(\operatorname{mod} q_1\right)$ so that we can originate

$$\mathfrak{W}_2' \equiv \boldsymbol{T}_b\left(\mathfrak{W}_1\right) \equiv \boldsymbol{T}_b\left(\boldsymbol{T}_{\mathrm{u}}(w)\right) \equiv \boldsymbol{T}_{\mathrm{u}}\left(\boldsymbol{T}_b(w)\right) \equiv \boldsymbol{T}_{\mathrm{u}}(p\mathrm{k}) \equiv \mathfrak{W}_2\left(\operatorname{mod} q_1\right)$$

and

$$\mathfrak{W}_4' \equiv \boldsymbol{T}_{\mathrm{u}}\left(\mathfrak{W}_3\right) \equiv \boldsymbol{T}_{\mathrm{u}}\left(\boldsymbol{T}_{\mathrm{v}}(w)\right) \equiv \boldsymbol{T}_{\mathrm{v}}\left(\boldsymbol{T}_{\mathrm{u}}(w)\right) \equiv \boldsymbol{T}_{\mathrm{v}}\left(\mathfrak{W}_1\right) \equiv \mathfrak{W}_4\left(\operatorname{mod} q_1\right).$$

As a result, the correctness of the scheme is established.

4.4 Password change stage

The smart card confirms the user's previously entered password before updating the newly updated password during this process. The user $\mathcal{U}_i$ goes through the following steps to update the password:

(1) Inserts the SC and suggestions both the $\boldsymbol{B}_i$ biometric template and pwd_i old password.

(2) $\boldsymbol{B}_i' = \boldsymbol{B}pwd \oplus \mathcal{H}\left(pwd_i\right)$ is computed by the smart card, and $\boldsymbol{B}_i = \boldsymbol{B}_i'$ is checked. If $\boldsymbol{B}_i \neq \boldsymbol{B}_i'$ is true, $\mathcal{U}_i$ has entered the incorrect old password or biometric template. The SC then declines the order.

(3) $\mathcal{U}_i$ enters their new password pwd_i^{new}, if the biometric verification is effective.

(4) The smart card is capable of computing the following:

$$\psi_i = \mathcal{H}\left(\boldsymbol{B}_i\right),$$

$$\mathcal{W}_i{}' = \mathcal{H}\left(pwd_i \parallel \boldsymbol{B}_i \parallel \mathrm{n}\right) \oplus \psi_i,$$

$$\mathcal{W}_i{}'' = \mathcal{H}\left(pwd_i{}^{new} \parallel \boldsymbol{B}_i \parallel \mathrm{n}\right) \oplus \psi_i,$$

$$\Omega_i{}' = \mathcal{Y}_i \oplus \mathcal{W}_i',$$

$$\mathcal{Y}_i{}' = \Omega_i{}' \oplus \mathcal{W}_i{}''.$$

(5) Finally, replaces $\mathcal{Y}_i$ with $\mathcal{Y}_i'$ on the smart card.

5 Security Analysis and Discussion

This segment contains a check to ensure that the procedure under consideration supports mutual authentication, perfect forward secrecy, and user anonymity. Furthermore, we tested the proposed protocol against a variety of attacks, including privileged insider attack, replay attack, offline password guessing attack, perfect forward secrecy, stolen-verifier attack, known-plaintext attack, and Bergamo et alattack.'s [56].

Proposition 1 *The proposed procedure can achieves privileged insider attacks.*

Proof The remote user $\mathcal{U}_i$ sends $\mathcal{H}\big(pwd_i \parallel \boldsymbol{B}_i \parallel \mathrm{n}\big)$ to the registration center $\mathcal{RC}_i$ during the registration procedure of the presented scheme. Without $\boldsymbol{B}_i$ and n, the privileged insider cannot deduce the password pwd_i. As a result, our system will withstand a privileged insider attack.

Proposition 2 *The presented procedure can achieve user anonymity.*

Proof The attacker can listen in on a user $\mathcal{U}_i$'s communication with a server $\mathcal{S}_i$ and attempt to track down the user's true identity to obtain info about the user. The real identity id_i is secured in our scheme by $\mathfrak{W}_2 \equiv \mathfrak{W}_2' \equiv \boldsymbol{T}_b\big(\boldsymbol{T}_{\mathrm{u}}(w)\big)\big(\bmod q_1\big)$ from $p\mathrm{k} \equiv \boldsymbol{T}_b(w)\big(\bmod q_1\big)$ and $\mathfrak{W}_1 \equiv \boldsymbol{T}_{\mathrm{u}}(w)\big(\bmod q_1\big)$. The attacker would need to deal with the convolution-Chebyshev chaotic maps-based DHP to compute $\mathfrak{m}_2$. As a result, our presented scheme will guarantee user anonymity.

Proposition 3 *The proposed procedure can achieves mutual authentication.*

Proof The mutual authentication among the user $\mathcal{U}_i$ and server $\mathcal{S}_i$ is possible with our presented scheme. To authenticate $\mathcal{U}_i$, server $\mathcal{S}_i$ must check the validity of γ and ξ during the authentication process of our presented scheme. To authenticate $\mathcal{S}_i$, the user $\mathcal{U}_i$'s smart card must also check the validity of μ. If an attacker attempts to forge messages, she/he will be faced with the convolution-Chebyshev chaotic maps-based DLP and the convolution-Chebyshev chaotic maps-based DHP. As a result, both the server and the user will authenticate, resulting in mutual authentication.

Proposition 4 *The presented procedure can achieve an off-line password guessing attack.*

Proof The messages $\{\mathrm{n}id_i, \mathfrak{W}_1, \gamma, \tau_1\}$ and $\{\mathfrak{W}_3, \mu, \tau_2\}$ may be intercepted by the attacker. The attacker can also gain access to the smart card's $\mathcal{Y}_i$. Then, she/he will try to guess the pwd_i' password. However, since the attacker lacks knowledge of the elements $\mathcal{W}_i$, ψ_i, $\boldsymbol{B}_i$ and Ω_i, the attacker is unable to check the correctness of the password pwd_i'. The attacker will also have to deal with the convolution-Chebyshev chaotic maps-based DHP if he tries to derive the random integers u and v. As a result, our system can withstand an offline password guessing attack.

Proposition 5 *The presented procedure can achieve replay attacks.*

Proof In the next run, the attacker might intercept contact messages from $\mathcal{U}_i$ and replay them to the server $\mathcal{S}_i$. With the wrong timestamps, however, the intruder is unable to pass the verification. So, by using the timestamps τ_1, τ_2, and τ_3, our presented procedure is safe against the replay attack.

Proposition 6 *The proposed procedure can achieves a stolen-verifier attack.*

Proof The stolen-verifier attack occurs when an intruder good deals with the server's security-sensitive verification table and uses it to impersonate a genuine user during the authentication process. In our presented system, the server does not need to keep any security-subtle verification tables. As a result, our procedure is immune to the stolen-verifier attack.

Proposition 7 *The projected procedure can achieve perfect forward secrecy.*

Proof According to perfect forward secrecy, even if a session key or long-term key is compromised in some way, the foe will be unable to extract all other session keys from the cracked one [61, 62]. In our proposed procedure, the smart card and server $\mathcal{S}_j$ compute the existing session key $\xi = \mathcal{H}\left(id_i \parallel \Omega_i' \parallel \mathfrak{W}_2 \parallel \mathfrak{W}_4 \parallel \tau_3\right)$, where $\mathfrak{W}_3 \equiv \boldsymbol{T}_{\mathrm{v}}(w)\left(\mathrm{mod}\, q_1\right)$, and $\mathfrak{W}_4 \equiv \boldsymbol{T}_{\mathrm{u}}\left(\mathfrak{m}_3\right)\left(\mathrm{mod}\, q_1\right)$ use random numbers v and u and $\Omega_i' = \mathcal{Y}_i \oplus \mathcal{W}_i'$, where $\mathcal{W}_i' = \mathcal{H}\left(pwd_i \parallel \boldsymbol{B}_i \parallel \mathrm{n}\right) \oplus \psi_i$. Even if a foe knew the current session key, they would be unable to use it to calculate any of the other valid session keys because the random numbers in each contact session are unique. With our presented procedure, this procedure aids in maintaining complete forward confidentiality.

Proposition 8 *The projected procedure can achieves lost smart card attacks.*

Proof Assume that a side-channel attack will remove all of the data from the smart card [63, 64]. The attacker may attempt to deduce the password from the data, but the elements protect the password $\mathcal{W}_i$, ψ_i, $\boldsymbol{B}_i$, and Ω_i, which the attacker does not have access to it. Furthermore, if the biometric template of the user $\boldsymbol{B}_i$, is not provided, the attacker is unable to pass biometric authentication. As a result, our presented procedure is impervious to smart card theft.

Proposition 9 *The presented procedure can achieves Bergamo et al.'s attack* [56].

Proof Bergamo et al.'s attack [56] is predicated on a foe being able to obtain the related variables b, w, $\mathfrak{W}_1$, and $\mathfrak{W}_3$ and derive u and v from them. The adversary may be able to quickly obtain b, w, $\mathfrak{W}_1$, and $\mathfrak{W}_3$, but there is no way in our presented procedure to extract u and v from those values. Convolution-Chebyshev chaotic maps encrypt the elements, which can only be identified by the client and server. In addition, we use enhanced convolution-Chebyshev chaotic maps to avoid the periodicity of the cosine function by extending the $\mathcal{Y}$ interval to $(-\infty, +\infty)$. As a result, Bergamo et al. attack's [56] have no bearing on our proposed procedure.

Table 3 Comparisons of security characteristics among the projected and other related procedures

Procedures Security characteristics	[65]	[61]	[66]	[67]	[33]	[34]	Proposed procedure
$\mathcal{SA}1$	ℵ	ℵ	𝒴	ℵ	ℵ	ℵ	𝒴
$\mathcal{SA}2$	ℵ	𝒴	𝒴	𝒴	𝒴	𝒴	𝒴
$\mathcal{SA}3$	𝒴	𝒴	𝒴	𝒴	𝒴	𝒴	𝒴
$\mathcal{SA}4$	𝒴	𝒴	𝒴	ℵ	ℵ	ℵ	𝒴
$\mathcal{SA}5$	𝒴	𝒴	𝒴	ℵ	𝒴	ℵ	𝒴
$\mathcal{SA}6$	ℵ	𝒴	𝒴	𝒴	𝒴	𝒴	𝒴
$\mathcal{SA}7$	ℵ	ℵ	ℵ	𝒴	ℵ	𝒴	𝒴
$\mathcal{SA}8$	ℵ	𝒴	𝒴	ℵ	𝒴	ℵ	𝒴
$\mathcal{SA}9$	ℵ	ℵ	ℵ	ℵ	ℵ	ℵ	𝒴

$\mathcal{SA}1$: privileged insider attack; $\mathcal{SA}2$: client anonymity; $\mathcal{SA}3$: Mutual authentication; $\mathcal{SA}4$: off-line password guessing attack; $\mathcal{SA}5$: replay attack; $\mathcal{SA}6$: stolen-verifier attack; $\mathcal{SA}7$: perfect forward secrecy; $\mathcal{SA}8$: lost FPROPOsmart card attack; $\mathcal{SA}9$: Bergamo et al.'s attack

y secure, ℵ vulnerable

6 Performance analysis and discussion

We demonstrate how well the proposed procedure works in this section of the paper. Table 3 compares the security futures of our projected procedure to those of Lee et al. [65], He et al. [61], Lee and Hsu [66], Fan et al. [67], Qi and Chen [33], and Sahoo et al. [34] existing procedures. Under critical considerations, our proposed procedure provides more security than the other existing procedures. Furthermore, we compared the computational primitives used in our proposed procedure for positioning the user and server to those used in other related procedures. We assume that the hash output of $h(.)$ is 160 bits (if we use the SHA-1 hash algorithm [68]) and that both the clear identity $\boldsymbol{id}_i^{\prime}$ and the check value are 160 bits. As a result, a sensor node's total storage requirement is 480 bits.

In this comparison, we used the four-time complexity notations: $\mathtt{t}_{ch}$, $\mathtt{t}_{s}$,$\mathtt{t}_{h}$, and $\mathtt{t}_{\mathrm{ec}}$ which described the performance time for a Chebyshev chaotic map operation, one elliptic curve scale multiplication, a one-way hash function, and a symmetric encryption/decryption operation, respectively. Several works [35–37, 69] have recognized the relationships between $\mathtt{t}_{\mathrm{h}}, \mathtt{t}_{\mathrm{ch}}, \mathtt{t}_{\mathrm{s}}$ and $\mathtt{t}_{\mathrm{ec}}$ with respect to $\mathtt{t}_{\mathrm{h}}$ $\left(\mathtt{t}_{\mathrm{h}} = 0.32\,\mathrm{ms}\right)$. The relationship and order of computational complexity among the metrics are as follows: $\mathtt{t}_{s} \approx \mathtt{t}_{h}, \mathtt{t}_{\mathrm{ch}} \approx \mathtt{t}_{\mathrm{h}}, \mathtt{t}_{\mathrm{ec}} \approx 72.5\mathtt{t}_{\mathrm{h}}$, and $\mathtt{t}_{ch} \approx \mathtt{t}_{\mathrm{h}} \approx \mathtt{t}_{\mathrm{s}} < \mathtt{t}_{\mathrm{ec}}$. Table 4 shows the proposed procedure as well as the most time-consuming operations of the existing procedures. Figure 7 also compares total processing costs in milliseconds (ms).

By comparison, due to the use of Chebyshev chaotic maps and hash functions, our proposed procedure can provide comprehensive security assurance at a very low computation cost while demonstrating very high efficiency.

Remote user authentication is an essential part of accessing valuable services or resources in healthcare, the Internet of Things (IoT), multi-server environments,

Table 4 Performance evaluation of the presented and other relevant procedures

Procedures	User ($\mathcal{U}_i$)	Server $\left(\mathcal{S}_i\right)$	Total
Lee et al. [65]	$6\mathtt{t}_h + 3\mathtt{t}_{ch}$	$7\mathtt{t}_h + 3\mathtt{t}_{ch}$	$13\mathtt{t}_h + 6\mathtt{t}_{ch}$
He et al. [61]	$7\mathtt{t}_h + 3\mathtt{t}_{ch}$	$7\mathtt{t}_h + 3\mathtt{t}_{ch}$	$13\mathtt{t}_h + 6\mathtt{t}_{ch}$
Lee and Hsu [66]	$10\mathtt{t}_h + 3\mathtt{t}_{ch}$	$7\mathtt{t}_h + 3\mathtt{t}_{ch}$	$17\mathtt{t}_h + 6\mathtt{t}_{ch}$
Fan et al. [67]	$8\mathtt{t}_h + 2\mathtt{t}_{ec} + 2\mathtt{t}_s$	$8\mathtt{t}_h + 2\mathtt{t}_{ec} + 2\mathtt{t}_s$	$16\mathtt{t}_h + 4\mathtt{t}_{ec} + 4\mathtt{t}_s$
Qi and Chen [33]	$11\mathtt{t}_h + 3\mathtt{t}_{ec} + 1\mathtt{t}_s$	$5\mathtt{t}_h + 3\mathtt{t}_{ec} + 1\mathtt{t}_s$	$16\mathtt{t}_h + 6\mathtt{t}_{ec} + 2\mathtt{t}_s$
Sahoo et al. [34]	$10\mathtt{t}_h + 4\mathtt{t}_{ec} + 1\mathtt{t}_s$	$5\mathtt{t}_h + 3\mathtt{t}_{ec} + 1\mathtt{t}_s$	$15\mathtt{t}_h + 7\mathtt{t}_{ec} + 2\mathtt{t}_s$
Proposed procedure	$6\mathtt{t}_h + 3\mathtt{t}_{ch}$	$5\mathtt{t}_h + 3\mathtt{t}_{ch}$	$11\mathtt{t}_h + 6\mathtt{t}_{ch}$

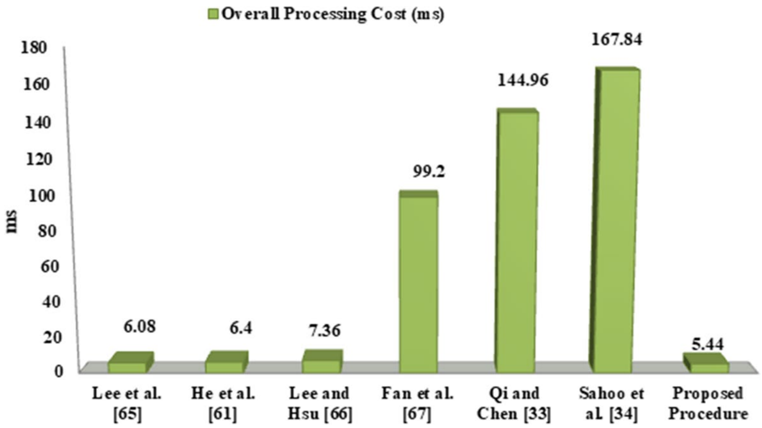

Fig. 7 Overall processing cost (ms)

and cloud applications. Remote user authentication [70] is an essential part of any security architecture. Authorization grants identity-based privileges, and audit trails are not transparent without authentication. The presented procedure is lightweight; therefore, it is very useful for the development of lightweight authentication protocols for Internet of Things (IoT), multi-server environments, and cloud applications.

The convolution is a mathematical operation on two functions, formulas (polynomials, expressions, etc.) (X and Y) that yields a third function X*Y=Z) that states how the outline of one is improved by the other. The term convolution indicates to both the consequence function and to the procedure of calculating it. Understanding discrete convolution as polynomial multiplication, which is a necessary operation in digital signal and image processing. The summation on k-times is known as a periodic summation of the function X with respect to Y. The proposed procedure is based on the convolution-Chebyshev chaotic maps and its security is based on the hardness of convolution-Chebyshev chaotic maps.

7 Conclusions

This article projected an efficient convolution-Chebyshev chaotic maps-enabled remote user authentication with key agreement procedure using biometric. We developed the extended convolution-Chebyshev chaotic maps over the interval $(-\infty, +\infty)$ and derived the required properties to establish the proposed procedure. The procedure shows significant biometric authentication without verification tables, enhances user anonymity, gives perfect forward secrecy, and has less computational and communication costs. Finally, formal and informal security and performance analyses revealed that the proposed procedure performs better than related procedures in the literature. Future work would focus on harnessing the potentials of the proposed procedure to provide a secure biometric authenticated key agreement for telemedicine-based information systems.

Acknowledgements The authors would like to thank anonymous reviewers of The Journal of Supercomputing for their careful and helpful comments and extend their gratitude to the Deanship of Scientific Research at King Khalid University for funding this work through the research groups program under Grant Number R. G. P. 2/150/42. The work of Agbotiname Lucky Imoize is supported by the Nigerian Petroleum Technology Development Fund (PTDF) and the German Academic Exchange Service (DAAD) through the Nigerian-German Postgraduate Program under Grant 57473408.

Author contributions Conceptualization was done by CM and RWI; Formal analysis was carried out by ALI; Investigation was done by CM; RWI; and ALI; Methodology was done by CM; RWI; and SSJ; Resources were done by CM; Software was done by SGM; ALI; and SKB; Supervision was done by CM; RWI; and ALI; Validation/Visualization were carried out by CM; SSJ; and RWI; Writing—original draft were done by CM; RWI; and SSJ; Writing—review and editing were carried out by CM; RWI; SSJ; SGM; ALI; and SKB.

Data availability No data was used in this article.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. Meshram C, Ibrahim RW, Meshram SG, Jamal SS, Imoize AL (2021) An efficient authentication with key agreement procedure using Mittag–Leffler–Chebyshev summation chaotic map under the multi-server architecture. J Supercomput. https://doi.org/10.1007/s11227-021-04039-1
2. Meshram C, Obaidat MS, Hsiao K-F, Imoize AL, Meshram A (2021) An effective fair off-line electronic cash protocol using extended chaotic maps with anonymity revoking trustee. In: 2021 International Conference on Communications, Computing, Cybersecurity, and Informatics, pp 1–5. https://doi.org/10.1109/ccci52664.2021.9583217
3. Lin C-H et al (2021) Intelligent symmetric cryptography with chaotic map and quantum based key generator for medical images infosecurity. IEEE Access 9:118624–118639
4. Kocarev L (2002) Chaos-based cryptography: a brief overview. IEEE Circ Syst Mag 1(3):6–21

5. Aydın Y, Özkaynak F (2021) Eligibility analysis of different chaotic systems derived from logistic map for design of cryptographic components. In: 2021 International Conference Engineering Technologies and Computer Science (EnT), pp 27–31
6. Munir N, Khan M, Hazzazi MM, Aijaedi A, Alharbi AR, Hussain I (2021) Cryptanalysis of internet of health things encryption scheme based on chaotic maps. IEEE Access 9:105678–105685
7. Imoize AL, Adedeji O, Tandiya N, Shetty S (2021) 6G enabled smart infrastructure for sustainable society: opportunities, challenges, and research roadmap. Sensors 21(5):1–58. https://doi.org/10.3390/s21051709
8. Li C-T, Hwang M-S (2010) An efficient biometrics-based remote user authentication scheme using smart cards. J Netw Comput Appl 33(1):1–5
9. Meshram C, Obaidat MS, Meshram A (2020) An efficient robust lightweight remote user authentication protocol using extended chaotic maps. In: Proceedings of the 2020 International Conference on Computer, Information, and Telecommunication Systems, CITS 2020, pp 8–13. https://doi.org/10.1109/CITS49457.2020.9232622
10. Sun Q, Moon J, Choi Y, Won D (2016) An improved dynamic ID based remote user authentication scheme for multi-server environment. In: Green, Pervasive, and Cloud Computing, pp 229–242
11. Lamport L (1981) Password authentication with insecure communication. Commun ACM 24(11):770–772
12. Fan L, Li J-H, Zhu H-W (2002) An enhancement of timestamp-based password authentication scheme. Comput Secur 21(7):665–667
13. Lee C-C (2009) On security of an efficient nonce-based authentication scheme for SIP. Int J Netw Secur 9(3):201–203
14. Shen J-J, Lin C-W, Hwang M-S (2003) Security enhancement for the timestamp-based password authentication scheme using smart cards. Comput Secur 22(7):591–595
15. Sarohi HK, Khan FU (2013) Graphical password authentication schemes: current status and key issues. Int J Comput Sci Issues 10(2 Part 1):437
16. Sun H-M, Chen Y-H, Lin Y-H (2011) oPass: a user authentication protocol resistant to password stealing and password reuse attacks. IEEE Trans Inf Forensics Secur 7(2):651–663
17. Lu Y, Li L, Peng H, Yang Y (2015) An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem. J Med Syst 39(3):1–8
18. Chaudhry SA, Naqvi H, Farash MS, Shon T, Sher M (2018) An improved and robust biometrics-based three factor authentication scheme for multiserver environments. J Supercomput 74(8):3504–3520
19. He D, Wang D (2014) Robust biometrics-based authentication scheme for multiserver environment. IEEE Syst J 9(3):816–823
20. Odelu V, Das AK, Goswami A (2015) A secure biometrics-based multi-server authentication protocol using smart cards. IEEE Trans Inf Forensics Secur 10(9):1953–1966
21. Jain AK, Ross A, Prabhakar S (2004) An introduction to biometric recognition. IEEE Trans Circuits Syst Video Technol 14(1):4–20
22. Li C-T, Hwang M-S (2010) An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards. Network 3(4):5
23. Maltoni D, Maio D, Jain AK, Prabhakar S (2009) Handbook of fingerprint recognition. Springer
24. Prabhakar S, Pankanti S, Jain AK (2003) Biometric recognition: security and privacy concerns. IEEE Secur Priv 1(2):33–42
25. Das AK (2011) Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards. IET Inf Secur 5(3):145–151
26. Chuang M-C, Chen MC (2014) An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics. Expert Syst Appl 41(4):1411–1418
27. Mishra D, Das AK, Mukhopadhyay S (2014) A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards. Expert Syst Appl 41(18):8129–8143
28. Lin H, Wen F, Du C (2015) An improved anonymous multi-server authenticated key agreement scheme using smart cards and biometrics. Wirel Pers Commun 84(4):2351–2362
29. Lu Y, Li L, Yang X, Yang Y (2015) Robust biometrics based authentication and key agreement scheme for multi-server environments using smart cards. PLoS ONE 10(5):e1026323
30. Mir O, Nikooghadam M (2015) A secure biometrics based authentication with key agreement scheme in telemedicine networks for e-health services. Wirel Pers Commun 83(4):2439–2461

31. Chaudhry SA, Naqvi H, Khan MK (2018) An enhanced lightweight anonymous biometric based authentication scheme for TMIS. Multimed Tools Appl 77(5):5503–5524
32. Zhu H, Zhang Y, Sun Y (2016) Provably secure multi-server privacy-protection system based on Chebyshev chaotic maps without using symmetric cryptography. Int J Netw Secur 18(5):803–815
33. Qi M, Chen J (2018) New robust biometrics-based mutual authentication scheme with key agreement using elliptic curve cryptography. Multimed Tools Appl 77(18):23335–23351
34. Sahoo SS, Mohanty S, Majhi B (2020) Improved biometric-based mutual authentication and key agreement scheme using ECC. Wirel Pers Commun 111(2):991–1017
35. Meshram C, Obaidat MS, Tembhurne JV, Shende SW, Kalare KW, Meshram SG (2020) A lightweight provably secure digital short-signature technique using extended chaotic maps for human-centered IoT systems. IEEE Syst J. https://doi.org/10.1109/JSYST.2020.3043358
36. Meshram C, Ibrahim RW, Obaid AJ, Meshram SG, Meshram A, Abd El-Latif AM (2021) Fractional chaotic maps based short signature scheme under human-centered IoT environments. J Adv Res 32:139–148
37. 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. https://doi.org/10.1109/ACCESS.2020.2991348
38. Meshram C, Li C-T, Meshram SG (2019) An efficient online/offline ID-based short signature procedure using extended chaotic maps. Soft Comput 23(3):747–753. https://doi.org/10.1007/s00500-018-3112-2
39. Meshram C, Ibrahim RW, Deng L, Shende SW, Meshram SG, Barve SK (2021) A robust smart card and remote user password-based authentication protocol using extended chaotic maps under smart cities environment. Soft Comput 25(15):10037–10051. https://doi.org/10.1007/s00500-021-05929-5
40. Meshram C, Obaidat MS, Meshram A (2020) An efficient robust lightweight remote user authentication protocol using extended chaotic maps. In: 2020 International Conference on Computer, Information and Telecommunication Systems (CITS), pp 1–6. https://doi.org/10.1109/CITS49457.2020.9232622
41. Zou L, Sun J, Gao M, Wan W, Gupta BB (2019) A novel coverless information hiding method based on the average pixel value of the sub-images. Multimed Tools Appl 78(7):7965–7980
42. Yu Z, Gao C, Jing Z, Gupta BB, Cai Q (2018) A practical public key encryption scheme based on learning parity with noise. IEEE Access 6:31918–31923
43. Yu C, Li J, Li X, Ren X, Gupta BB (2018) Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer generated hologram. Multimed Tools Appl 77(4):4585–4608
44. 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):1–15. https://doi.org/10.1002/dac.4307
45. Meshram C, Lee C-C, Meshram SG, Li C-T (2019) An efficient ID-based cryptographic transformation model for extended chaotic-map-based cryptosystem. Soft Comput 23(16):6937–6946. https://doi.org/10.1007/s00500-018-3332-5
46. Premkamal PK, Pasupuleti SK, Alphonse PJA (2020) Efficient escrow-free CP-ABE with constant size ciphertext and secret key for big data storage in cloud. Int J Cloud Appl Comput 10(1):28–45
47. Zheng Q, Wang X, Khan MK, Zhang W, Gupta BB, Guo W (2017) A lightweight authenticated encryption scheme based on chaotic SCML for railway cloud service. IEEE Access 6:711–722
48. Kumar A (2019) Design of secure image fusion technique using cloud for privacy-preserving and copyright protection. Int J Cloud Appl Comput 9(3):22–36
49. Meshram C, Ibrahim RW, Obaidat MS, Sadoun B, Meshram SG, Tembhurne JV (2021) An effective mobile-healthcare emerging emergency medical system using conformable chaotic maps. Soft Comput 25(14):8905–8920. https://doi.org/10.1007/s00500-021-05781-7
50. Poongodi M, Malviya M, Hamdi M, Vijayakumar V, Mohammed MA, Rauf HT, Al-Dhlan KA (2021) 5G based Blockchain network for authentic and ethical keyword search engine. IET Commun. https://doi.org/10.1049/cmu2.12251
51. Mohammed MA, Ibrahim DA, Salman AO (2021) Adaptive intelligent learning approach based on visual anti-spam email model for multi-natural language. J Intell Syst 30(1):774–792
52. Awan MJ et al (2021) Image-based malware classification using VGG19 network and spatial convolutional attention. Electronics 10(19):2444
53. Li Z, Zhao M, Jiang H, Xu Q (2019) Keyword guessing on multi-user searchable encryption. Int J High Perform Comput Netw 14(1):60–68

54. Gaikwad VP, Tembhurne JV, Meshram C, Lee C-C (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
55. Mason JC, Handscomb DC (2002) Chebyshev polynomials. CRC Press
56. 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. https://doi.org/10.1109/TCSI.2005.851701
57. Han S, Chang E (2009) Chaotic map based key agreement with/out clock synchronization. Chaos Solitons Fract 39(3):1283–1289. https://doi.org/10.1016/j.chaos.2007.06.030
58. Zhang L (2008) Cryptanalysis of the public key encryption based on multiple chaotic systems. Chaos Solitons Fract 37(3):669–674. https://doi.org/10.1016/j.chaos.2006.09.047
59. Chen F, Liao X, Wong K, Han Q, Li Y (2012) Period distribution analysis of some linear maps. Commun Nonlinear Sci Numer Simul 17(10):3848–3856
60. Laine TP (1980) The product formula and convolution structure for the generalized Chebyshev polynomials. SIAM J Math Anal 11(1):133–146
61. 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. https://doi.org/10.1007/s11071-012-0335-0
62. He D, Ma M, Zhang Y, Chen C, Bu J (2011) A strong user authentication scheme with smart cards for wireless communications. Comput Commun 34(3):367–374. https://doi.org/10.1016/j.comcom.2010.02.031
63. Kocher P, Jaffe J, Jun B (1999) Differential power analysis. In: Annual International Cryptology Conference, pp 388–397
64. 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
65. Lee C-C, Chen C-L, Wu C-Y, Huang S-Y (2012) An extended chaotic maps-based key agreement protocol with user anonymity. Nonlinear Dyn 69(1):79–87. https://doi.org/10.1007/s11071-011-0247-4
66. Lee C-C, Hsu C-W (2013) A secure biometric-based remote user authentication with key agreement scheme using extended chaotic maps. Nonlinear Dyn 71(1):201–211. https://doi.org/10.1007/s11071-012-0652-3
67. Wu F, Xu L, Kumari S, Li X (2015) A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client–server networks. Comput Electr Eng 45:274–285
68. Secure Hash Standard, National Institute of Standards and Technology (NIST), Federal Information Processing Standards Publication. FIPS 180-4, 2015
69. Ibrahim MH, Kumari S, Das AK, Wazid M, Odelu V (2016) Secure anonymous mutual authentication for star two-tier wireless body area networks. Comput Methods Programs Biomed 135:37–50
70. Park Y, Park K, Lee K, Song H, Park Y (2017) Security analysis and enhancements of an improved multi-factor biometric authentication scheme. Int J Distrib Sens Netw 13(8):1–12

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

Chandrashekhar Meshram[1] · Rabha W. Ibrahim[2] · Sarita Gajbhiye Meshram[3] · Agbotiname Lucky Imoize[4,5] · Sajjad Shaukat Jamal[6] · Sharad Kumar Barve[3]

Rabha W. Ibrahim
rabhaibrahim@yahoo.com

Sarita Gajbhiye Meshram
gajbhiyesarita@gmail.com

Agbotiname Lucky Imoize
aimoize@unilag.edu.ng

Sajjad Shaukat Jamal
shussain@kku.edu.sa

Sharad Kumar Barve
drsharadbarve@gmail.com

[1] Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar Government Post-Graduation College, College of Chhindwara University, Betul, M.P. 460001, India

[2] IEEE: 94086547, 59200 Kuala Lumpur, Malaysia

[3] Water Resources and Applied Mathematics Research Lab, Nagpur 440027, India

[4] Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Lagos, Akoka 100213, Lagos, Nigeria

[5] Department of Electrical Engineering and Information Technology, Institute of Digital Communication, Ruhr University, 44801 Bochum, Germany

[6] Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia