Computers, Materials & Continua
DOI: 10.32604/cmc.2022.024996
Article

Tech Science Press

An Efficient Three-Factor Authenticated Key Agreement Technique Using FCM Under HC-IoT Architectures

Chandrashekhar Meshram[1,*], Agbotiname Lucky Imoize[2,3], Sajjad Shaukat Jamal[4], Parkash Tambare[5], Adel R. Alharbi[6] and Iqtadar Hussain[7]

[1]Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar Government Post-Graduation College, College of Chhindwara University, Betul, 460001, M.P., India
[2]Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Lagos, Akoka, Lagos, 100213, Nigeria
[3]Department of Electrical Engineering and Information Technology, Institute of Digital Communication, Ruhr University, 44801, Bochum, Germany
[4]Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia
[5]Water Resources & Applied Mathematics Research Lab, Nagpur, 440027, India
[6]College of Computing and Information Technology, University of Tabuk, Tabuk, 71491, Saudi Arabia
[7]Mathematics Program, Department of Mathematics, Statistics and Physics, College of Arts and Sciences, Qatar University, 2713, Doha, Qatar
*Corresponding Author: Chandrashekhar Meshram. Email: cs_meshram@rediffmail.com

Received: 07 November 2021; Accepted: 31 December 2021

Abstract: The Human-Centered Internet of Things (HC-IoT) is fast becoming a hotbed of security and privacy concerns. Two users can establish a common session key through a trusted server over an open communication channel using a three-party authenticated key agreement. Most of the early authenticated key agreement systems relied on pairing, hashing, or modular exponentiation processes that are computationally intensive and cost-prohibitive. In order to address this problem, this paper offers a new three-party authenticated key agreement technique based on fractional chaotic maps. The new scheme uses fractional chaotic maps and supports the dynamic sensing of HC-IoT devices in the network architecture without a password table. The projected security scheme utilized a hash function, which works well for the resource-limited HC-IoT architectures. Test results show that our new technique is resistant to password guessing attacks since it does not use a password. Furthermore, our approach provides users with comprehensive privacy protection, ensuring that a user forgery attack causes no harm. Finally, our new technique offers better security features than the techniques currently available in the literature.

Keywords: Three-party authenticated key agreement; anonymity; fractional chaotic maps; Chebyshev polynomial; password table; human-centered internet of things (HC-IoT)

1 Introduction

Security and privacy issues are fast proliferating the Human-Centered Internet of Things (HC-IoT) space [1]. As billions of user data are being collected and transmitted by IoT devices via open channels, the vulnerability of user data to adversarial attacks needs to be considered and addressed appropriately. Unauthorized users can gain real-time access to the HC-IoT devices unlawfully. Consequently, sensitive user data is compromised, leading to a catastrophic disruption of safety-critical processes under HC-IoT architectures. Therefore, the need for secure authenticated key agreement protocols to mitigate the vast security and privacy issues in HC-IoT systems cannot be overemphasized.

Several user authentications and key agreement techniques have been reported for HC-IoT systems [2]. Generally, the HC-IoT devices are resource-limited [3]. Therefore, applying complex cryptographic primitives to these devices is quite challenging due to their resource constraints. Some authors have proposed Elliptic Curve Cryptography (ECC) to guarantee secure session keys between legitimate users in IoT environments [4–6]. However, HC-IoT devices cannot support ECC operations due to limited storage and computational resources. In order to address this problem, lightweight authentication and key agreement schemes have been proposed [5,7,8]. It is worth mentioning that most of these schemes are specially designed to reduce the computational and communication costs inherent in the ECC schemes.

Authentication schemes can support fast computational processing of user information and low communication costs. However, most of these security schemes are susceptible to various attacks and cannot provide critical security requirements [8,9]. Thus, the problem of improving the authentication efficiency and simultaneously guaranteeing the security and privacy of the scheme remains. In order to solve this problem, our work presents an efficient three-factor authenticated key agreement technique using fractional chaotic maps under the HC-IoT architectures without a password table.

1.1 Motivation

In recent years, several studies have reported the prevalent security and privacy issues in HC-IoT architectures. Generally, these architectures communicate over public channels, which are vulnerable to several attacks inside and outside the networks. In particular, sensitive user information can be compromised when a malicious user unlawfully intercepts or accesses the HC-IoT devices [9]. Thus, it is imperative to adequately secure user authentication schemes to mitigate unscrupulous access to critical user data. In this case, the identities of all network users would require validation in real-time and access is denied to unauthorized users. In related works, a one-way cryptographic algorithm, a hash function, has been used to map input of any size to an individual output of a fixed length of bits. This helps to provide data integrity and guarantee security against unauthorized access.

In the preliminary schemes, only one HC-IoT device can be accessed by a particular user at a time. Thus, repeated user identity validation is required to access multiple sensing HC-IoT devices. However, this approach is time-consuming and cost-prohibitive to implement in practice. Therefore, the need for a three-factor authenticated key agreement technique using fractional chaotic maps to access several sensing devices in real-time without a password table and establish the shared session key among the network users is not out of place.

1.2 Contribution

This work presents an efficient three-factor authenticated key agreement technique using fractional chaotic maps under HC-IoT architectures. The following is a list of the paper's contributions.

- We present a secret sharing technique for constructing a secure three-factor authenticated key agreement without a password table. The presented technique utilized a hash function, which works well for the resource-limited HC-IoT devices.
- We establish the formal security proof of the presented technique using Burrows–Abadi–Needham (BAN) logic under random oracle. Specifically, our scheme differentiates a real adversary from a simulation.
- The three-factor authenticated key agreement technique designed using fractional chaotic maps supports the architecture's dynamic sensing of HC-IoT devices without a password table.
- Finally, we present a security investigation and performance comparison of the presented technique and demonstrate that it reduces the communication and computational overhead drastically compared to existing related techniques.

1.3 Paper Organization

The rest of this paper is laid out as follows. In Section 2, we present the related works. Section 3 gives the preliminaries covering fractional chaotic maps and their cryptographic properties. Section 4 focuses on the proposed technique under HC-IoT architectures. Section 5 deals with the formal authentication proof of the scheme using BAN logic. Section 6 presents the security investigation of the technique and valuable discussions. Section 7 covers the performance comparison of the presented technique to demonstrate its superiority over the existing schemes. Section 8 wraps up the paper with a concise conclusion.

2 Related Work

Distributed private cloud servers store critical user information harvested from HC-IoT devices to allow access to legitimate users. Several authentication protocols with a key agreement for use under HC-IoT architectures have been proposed [10–12]. In particular, a lightweight authentication scheme for application in Wireless Sensors Networks (WSNs) was proposed by Das [10]. The scheme allows users to validate their identities by entering their secret passwords and smart cards. However, the scheme uses only the hash function, limiting its security.

Additionally, some flaws have been identified in Das' scheme. These include the inability to resist denial-of-service attacks and node compromised attacks [11]. In order to address these limitations in Das' scheme, an authentication scheme utilizing biohacking has been proposed by [11]. The scheme gives a lower error rate compared to existing traditional techniques. However, Wang et al. [12] estimated several two-factor authentication techniques. They observed that the technique by Srinivas et al. [11] is susceptible to offline guessing attacks and cannot guarantee user anonymity in real-time.

In related work, Esfahani et al. [13] anticipated an efficient authentication technique using the hash function and exclusive OR (XOR) operation. The technique was tailored for application in the Industrial Internet of Things (IIoT). The technique achieves low communication and computational costs and satisfies several security requirements. In another related work, Wazid et al. [14] presented a user authentication and key management technique that uses passwords, biometrics and a smart card for identity validation. Hossain et al. [15] proposed a cloud-assisted scheme that gives real-time patient data for healthcare applications. In work due to Li et al. [4], elliptic curve cryptography (ECC)-empowered authentication protocol was proposed. The scheme seeks to tackle the security flaws in existing schemes and enhance IIoT wireless networks' privacy.

In another study, Li et al. [16] put forward a three-factor authentication technique for IIoT systems. The work aims at enhancing the security of the scheme to withstand sophisticated attacks and provide user anonymity. On integrating IoT with cloud computing to support IoT services, Yu et al. [17] demonstrated the possibility of achieving improved user services, leveraging IoT. However, several attacks that limit the security of cloud-based servers have been identified [18, 19]. Furthermore, the work [19] proposes a better authentication scheme, which applies to Internet of Things (IoT)-assisted cloud computing architectures to resist DoS and privileged insider attacks.

In [20], chaotic maps enabled authentication scheme was proposed for ID-based digital signatures. The security of the scheme was tested on the suppositions of complex Diffie-Hellman problems and discrete logarithm. Also, Gao et al. [21] put forward an authentication technique leveraging chaotic maps for the wireless body area networks. The technique facilitated the securely monitoring and recording of patients' health data. Performance analysis of the technique guarantees user confidentiality, and it reduces the cost of multiplication and exponentiation during computation at a low communication cost.

In a similar vein, an anonymity preserving authentication technique was proposed in [22]. Security verification of the technique was done using the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. Test results showed enhanced performances compared to other related techniques in the literature. In several works due to Meshram et al. [3,9,23], efficient and provably secure authentication techniques using extended chaotic maps were proposed. The schemes show robust security features covering low computational and communication costs.

In comparison with preceding techniques, the three-factor authenticated key agreement technique projected in this paper is unique in several aspects. The launched security scheme utilized a hash function, which works well for the resource-limited HC-IoT architectures. Finally, the technique uses fractional chaotic maps and supports the dynamic sensing of HC-IoT devices in the architecture without a password table.

3 Background and Material

Before going into the current inquiry on the presented three-factor authenticated key agreement technique, this part discusses the many fundamental principles pertaining to the work. First, a Chebyshev chaotic map implementation with a short existence is described. Following that, a Chebyshev polynomial, fractional chaotic maps utilizing the minimum approach, and a list of other techniques employed in this development are represented. The notations used in our method are briefly defined in Tab. 1.

Table 1: Notations used in our proposed scheme

Notations	Descriptions
$\mathcal{U}, \mathcal{V}$	Two participants
$\mathcal{S}$	The trusted server
$\mathrm{T}^{y}_{k}(id_{\mathcal{X}})$	Certificate of users allotted by the server
k	Secret key k of the server $\mathcal{S}$
$h()$	A chaotic map-based one-way hash function
$\mathcal{D}_{\kappa}()/\mathcal{E}_{\kappa}()$	Secure symmetric decryption/encryption functions with key κ
$id_{\mathcal{U}},\ id_{\mathcal{V}}$	$\mathcal{U}$'s and $\mathcal{V}$'s identity

3.1 Chebyshev Chaotic Maps

Two fundamental prerequisites in the evolution of cryptographic systems are ambiguity and dispersion. Chaotic frameworks are suitable for achieving diffusion and uncertainty assets in cryptography because of their sensitivity to primary conditions, ergodicity, and pseudo-randomness. As a result, chaotic maps have been used to create several symmetric and asymmetric key cryptosystems [24–26]:

Definition 1. (Chaotic map). In the variation v, the Chebyshev polynomial (CP) $Ͳ_n(ʋ)$ is an n-degree polynomial. Assume that $ʋ \in [-1,\ 1]$ is the edition and that n is a big integer. The following is what CP said in general [24,27–29]:

$$Ͳ_n(ʋ) = cos(n\ \ arccos(ʋ)), Ͳ_0(ʋ) = 1, Ͳ_1(ʋ) = ʋ$$

The Chebyshev polynomial's recurrence relation is defined as

$$Ͳ_n(ʋ) = 2ʋͲ_{n-1}(ʋ) - Ͳ_{n-2}(ʋ);\ n \geq 2$$

In this scenario, the functional $arccos(ʋ)$ and $cos(ʋ)$ are written as $arccos : [-1,\ 1] \to [0,\ ]$ and $cos : R \to [-1,\ 1]$.

3.1.1 Properties of Chaotic Maps

Chebyshev polynomials have the following two essential properties:

Chaotic properties*:* The CP transform $Ͳ_n : [-1,\ 1] \to\ \ [-1,\ 1]$ with the degree $n\ >\ 1$ is known as the chaotic maps transform. It is related to the functional (invariant density) $f^*(ʋ) = \frac{1}{\left(\pi\sqrt{1-ʋ^2}\right)}$ for some positive Lyapunov exponent $\lambda =$ In $n\ >\ 0$.

Semi-group properties: The semigroup property of $Ͳ_n(ʋ)$ is defined as follows: $Ͳ_\tau\ \ (Ͳ_l(ʋ))\ \ = cos(\tau\ cos^{-1}(cos(l\ cos^{-1}(ʋ))))\ \ =\ \ cos(\tau l\ cos^{-1}(ʋ))\ \ =\ \ Ͳ_{l\tau}(ʋ)\ \ =\ \ Ͳ_l(Ͳ_\tau\ (ʋ))$, where τ and l are positive integers and $ʋ \in [-1,\ 1]$.

Public-key cryptography based on the Chebyshev polynomial map semigroup property is unstable, according to Bergamo et al. [25]. Zhang [26] proved, however, that the semigroup property retains an interval $(-\infty, +\infty)$, which can improve the property as measured:

$$Ͳ_n(ʋ) = 2ʋͲ_{n-1}(ʋ) - Ͳ_{n-2}(ʋ)(mod\ q_1);\ n \geq 2$$

where q_1 is a big prime and $ʋ\ \in\ (-\infty, +\infty)$. As a result, the property is: $Ͳ_\tau(Ͳ_l(ʋ))(modq_1)\ = Ͳ_{l\tau}(ʋ)(modq_1) = Ͳ_l(Ͳ_\tau(ʋ))(modq_1)$, and the semigroup property is kept as well. It is worth noting that extended Chebyshev polynomials commute under confirmation as well.

3.1.2 Computational Problems

By using the propositions [27–31], various computational challenges based on Chebyshev polynomials are explained in this segment.

Definition 2. (Chaotic Map-based Discrete Logarithm Problem (CMDLP)). Any polynomial time-bounded technique that discovers the number τ where $y = Ͳ_\tau(ʋ)\ (mod\ q_1)$ is infeasible given a random tuple $\langle y,\ ʋ\rangle$.

Definition 3. (Chaotic Map-based Diffie-Hellman problem (CMDHP)). Any polynomial time-bounded procedure that attempts to find the estimate $Ͳ_{\tau l}(ʋ)\ (mod\ q_1)$ for a given random tuple $<ʋ$, $Ͳ_\tau(ʋ),\ T_l(ʋ) >$ fails.

3.2 Fractal Chaotic Maps (FCM)

Historically, the Fractal Calculus (FC) was called a local fractional calculus [32,33]. However, fractional calculus accepts possessions (derivatives of non-integer power). FC takes precedence over the related preparation:

Assume that the formal expression for a random fractional-order $\mu\epsilon$ [0, 1] defines the fractional difference operator ξ^{μ}. Then,

$$\xi^{\mu}\psi(z)=\frac{\Delta^{\mu}\ (\psi(z)-\psi(z_0))}{(z-z_0)^{\alpha}}=\Gamma(\mu+1)(\psi(z)-\psi(z_0))$$

and the fractal integral operator is the same as this.

$$I^{\mu}\psi(z)=\frac{1}{\Gamma(\mu+1)}\int_a^b\psi(z)(dz)^{\mu}.$$

It can be approximated using the formula in (1)

$$I^{\mu}\psi(z)=\frac{(b-a)^{\mu}}{\Gamma(\mu+1)}\ \psi(z),\qquad a\le z\le b. \tag{1}$$

We get the following formulation (2) by generalising the polynomial $\mathrm{T}_n(v)$, with the FC concept:

$$I^{\mu}\mathrm{T}_n(v):=\mathrm{T}_n^{\ \mu}(v)=\frac{(2)^{\mu}}{\Gamma(\mu+1)}\mathrm{T}_n(v), \tag{2}$$

The FCP stands for the fractal Chebyshev polynomial (see Fig. 1).

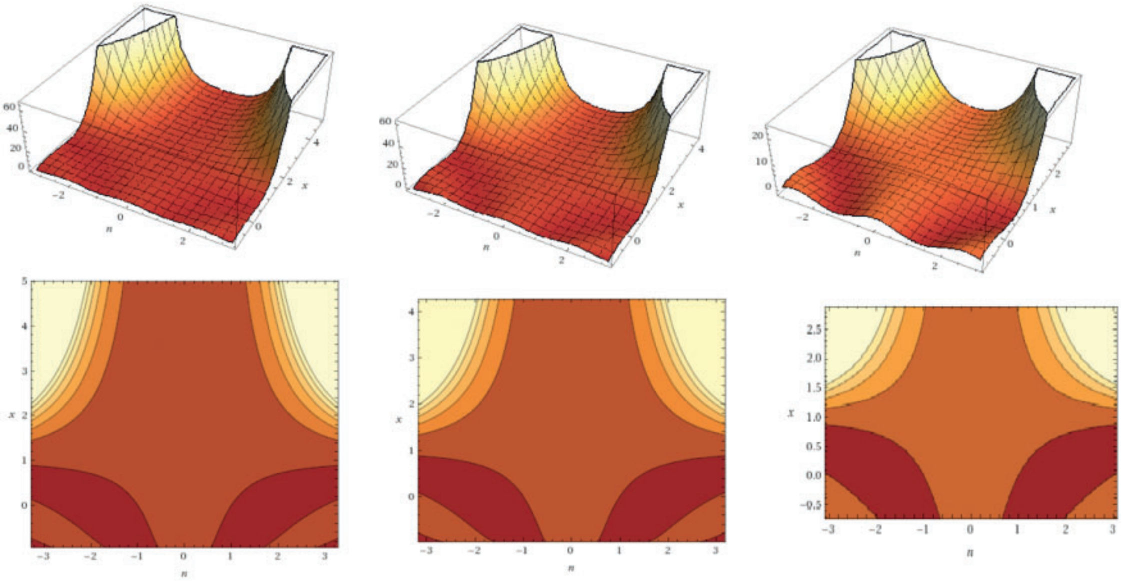

Figure 1: 3D-FCP when $\mu = 0$, 1/2 and 3/4 respectively

3.2.1 Properties of Fractal Chaotic Maps

Two of the FCP's soothing properties are as follows:

***Definition 4** (Chaotic possessions of FCM)*. The fractal Chaotic maps [33,34] satisfy the recurrent relations under the chaotic possessions, i.e., $T_n^{\mu}(v) = \frac{(2)^{\mu}}{\Gamma(\mu+1)}(2vT_{n-1}(v) - T_{n-2}(v))\ (mod\ q_1)$. When $\mu \to 0$ is utilized, the usual prominent effect, as observed in Yang et al. [32], is well understood.

Definition 5 (*Semi-group possessions of FCM*). The semi-group possessions hold, i.e., for FCMs on the interval $(-\infty, \infty)$ [33].

$$T_k^{\mu}(T_n^{\mu}(v))\ (mod\ q_1) = T_n^{\mu}(T_k^{\mu}(v))\ (mod\ q_1) = T_{kn}^{\mu}(v).\ (mod\ q_1)$$

4 The Proposed Technique Under the HC-IoT Architecture

This section will show you the steps of our new three-party authenticated key agreement technique. Fig. 2 depicts the layout of our strategy. Please note that the term $\mathcal{U} \to \mathcal{V}: (M)$ is used in all five phases to indicate that $\mathcal{U}$ deliver a message to $\mathcal{V}$. Our plan consists of five steps, which are outlined in Tab. 2 as follows.

Table 2: The steps of our new three-party authenticated key agreement technique

Steps	Description
Step 1: $\mathcal{U} \to \mathcal{V}: (M_1)$	User $\mathcal{U}$ picks r and calculates $\kappa_{\mathcal{US}} = T_r^{\gamma}T_k^{\gamma}(id_{\mathcal{U}})$, $H_{\mathcal{U}} = h(T_r^{\gamma}(id_{\mathcal{U}}) \parallel id_{\mathcal{U}} \parallel id_{\mathcal{V}})$, and $C_{\mathcal{U}} = \mathcal{E}_{\kappa_{\mathcal{US}}}(id_{\mathcal{U}} \parallel id_{\mathcal{V}} \parallel H_{\mathcal{U}} \parallel T_r^{\gamma}(id_{\mathcal{V}}))$ and then sends $M_1 = \{T_r^{\gamma}(id_{\mathcal{U}}),\ C_{\mathcal{U}}\}$ to $\mathcal{V}$.
Step 2: $\mathcal{V} \to \mathcal{S}: (M_1,\ M_2)$	Upon getting M_1 form $\mathcal{U}$, User $\mathcal{V}$ selects w and calculates $\kappa_{\mathcal{VS}} = T_w^{\gamma}T_k^{\gamma}(id_{\mathcal{V}})$, $H_{\mathcal{V}} = h(T_w^{\gamma}(id_{\mathcal{V}}) \parallel id_{\mathcal{V}})$, and $C_{\mathcal{V}} = \mathcal{E}_{\kappa_{\mathcal{VS}}}(id_{\mathcal{V}} \parallel H_{\mathcal{V}} \parallel T_w^{\gamma}(id_{\mathcal{V}}))$and then sends M_1 and $M_2 = \{T_w^{\gamma}(id_{\mathcal{V}}),\ C_{\mathcal{V}}\}$ to $\mathcal{S}$.
Step 3: $\mathcal{S} \to \mathcal{V}: (C'_{\mathcal{U}},\ C'_{\mathcal{V}})$	Upon getting $M_1,\ M_2$ form $\mathcal{V}$, the server $\mathcal{S}$ first calculates $\kappa_{\mathcal{SU}} = T_k^{\gamma}T_r^{\gamma}(id_{\mathcal{U}})$, $\kappa_{\mathcal{SV}} = T_k^{\gamma}T_w^{\gamma}(id_{\mathcal{V}})$, $\mathcal{D}_{\mathcal{U}} = \mathcal{D}_{\kappa_{\mathcal{SU}}}(C_{\mathcal{U}}) = \{id_{\mathcal{U}} \parallel id_{\mathcal{V}} \parallel H_{\mathcal{U}} \parallel T_r^{\gamma}(id_{\mathcal{V}})\}$, and $\mathcal{D}_{\mathcal{V}} = \mathcal{D}_{\kappa_{\mathcal{SV}}}(C_{\mathcal{V}}) = \{id_{\mathcal{V}} \parallel H_{\mathcal{V}} \parallel T_w^{\gamma}(id_{\mathcal{V}})$. Then $\mathcal{S}$ checks $id_{\mathcal{U}}$, $id_{\mathcal{V}}$, $H_{\mathcal{U}} =?h(T_r^{\gamma}(id_{\mathcal{U}}) \parallel id_{\mathcal{U}} \parallel id_{\mathcal{V}})$, and $H_{\mathcal{V}} =?h(T_w^{\gamma}(id_{\mathcal{V}}) \parallel id_{\mathcal{V}})$. If both checks out, $\mathcal{S}$ calculates $H_{\mathcal{SU}} = h(T_k(id_{\mathcal{U}}) \parallel T_r^{\gamma}(id_{\mathcal{U}}))$, $H_{\mathcal{SV}} = h(T_k^{\gamma}(id_{\mathcal{V}}) \parallel T_w^{\gamma}(id_{\mathcal{V}}))$, $C'_{\mathcal{U}} = \mathcal{E}_{\kappa_{\mathcal{SU}}}(id_{\mathcal{U}} \parallel id_{\mathcal{V}} \parallel T_w^{\gamma}(id_{\mathcal{V}}) \parallel H_{\mathcal{SU}})$, and $C'_{\mathcal{V}} = \mathcal{E}_{\kappa_{\mathcal{SV}}}(id_{\mathcal{U}} \parallel id_{\mathcal{V}} \parallel T_r^{\gamma}(id_{\mathcal{U}}) \parallel H_{\mathcal{SV}})$. After calculating $C'_{\mathcal{U}}$ and $C'_{\mathcal{V}}$, $\mathcal{S}$ sends them to $\mathcal{V}$.
Step 4: $\mathcal{V} \to \mathcal{U}: (C'_{\mathcal{U}},\ H_{\mathcal{VU}})$	Upon getting $C'_{\mathcal{U}}$ and $C'_{\mathcal{V}}$ from $\mathcal{S}$, $\mathcal{V}$ first decrypts $C'_{\mathcal{V}}$ and checks $id_{\mathcal{U}}$ and $H_{\mathcal{SV}}$. Then $\mathcal{V}$ calculates $\mathcal{S}\kappa = T_w^{\gamma}T_r^{\gamma}(id_{\mathcal{V}})$ and $H_{\mathcal{VU}} = h(\mathcal{S}\kappa \parallel C'_{\mathcal{U}})$. After calculating $H_{\mathcal{VU}}$, $\mathcal{V}$ sends $C'_{\mathcal{U}}$ and $H_{\mathcal{VU}}$ to $\mathcal{U}$.
Step 5: $\mathcal{U} \to \mathcal{V}: (H_{\mathcal{UV}})$	Upon getting $C'_{\mathcal{U}}$ and $H_{\mathcal{VU}}$ from $\mathcal{V}$, $\mathcal{U}$ first decrypts $C'_{\mathcal{U}}$ and checks $H_{\mathcal{SU}}$. Then $\mathcal{U}$ calculates $\mathcal{S}\kappa = T_r^{\gamma}T_w^{\gamma}(id_{\mathcal{V}})$. After calculating $\mathcal{S}\kappa$, $\mathcal{U}$ checks $H_{\mathcal{VU}} =?h(\mathcal{S}\kappa \parallel C'_{\mathcal{U}})$. If positive, $\mathcal{U}$ calculates $H_{\mathcal{UV}} = h(\mathcal{S}\kappa \parallel id_{\mathcal{U}} \parallel T_r^{\gamma}(id_{\mathcal{V}}))$ and sends it to $\mathcal{V}$. Upon getting $H_{\mathcal{UV}}$ from $\mathcal{U}$, $\mathcal{V}$ approves $H_{\mathcal{UV}}$. The session key between $\mathcal{U}$ and $\mathcal{V}$ will be $\mathcal{S}\kappa' = h(\mathcal{S}\kappa)$ if it checks out.

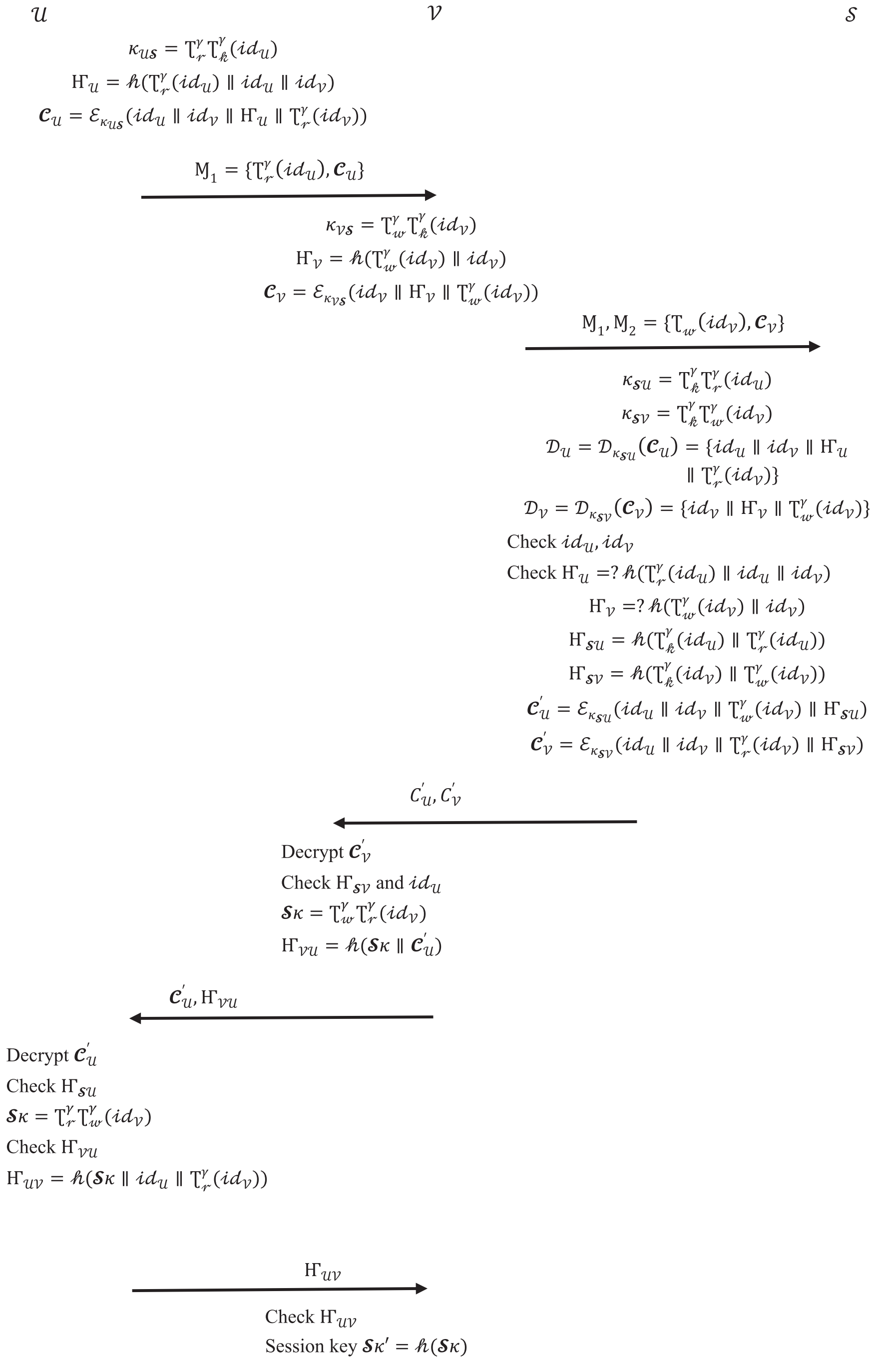
$\mathcal{U}$
$\mathcal{V}$
$\mathcal{S}$
$\kappa_{\mathcal{US}} = \mathrm{T}_r^{\gamma}\mathrm{T}_k^{\gamma}(id_{\mathcal{U}})$
$\mathrm{H}_{\mathcal{U}} = \hbar(\mathrm{T}_r^{\gamma}(id_{\mathcal{U}}) \parallel id_{\mathcal{U}} \parallel id_{\mathcal{V}})$
$\mathcal{C}_{\mathcal{U}} = \mathcal{E}_{\kappa_{\mathcal{US}}}(id_{\mathcal{U}} \parallel id_{\mathcal{V}} \parallel \mathrm{H}_{\mathcal{U}} \parallel \mathrm{T}_r^{\gamma}(id_{\mathcal{V}}))$
$\mathrm{M}_1 = \{\mathrm{T}_r^{\gamma}(id_{\mathcal{U}}), \mathcal{C}_{\mathcal{U}}\}$
$\kappa_{\mathcal{VS}} = \mathrm{T}_w^{\gamma}\mathrm{T}_k^{\gamma}(id_{\mathcal{V}})$
$\mathrm{H}_{\mathcal{V}} = \hbar(\mathrm{T}_w^{\gamma}(id_{\mathcal{V}}) \parallel id_{\mathcal{V}})$
$\mathcal{C}_{\mathcal{V}} = \mathcal{E}_{\kappa_{\mathcal{VS}}}(id_{\mathcal{V}} \parallel \mathrm{H}_{\mathcal{V}} \parallel \mathrm{T}_w^{\gamma}(id_{\mathcal{V}}))$
$\mathrm{M}_1, \mathrm{M}_2 = \{\mathrm{T}_w(id_{\mathcal{V}}), \mathcal{C}_{\mathcal{V}}\}$
$\kappa_{\mathcal{SU}} = \mathrm{T}_k^{\gamma}\mathrm{T}_r^{\gamma}(id_{\mathcal{U}})$
$\kappa_{\mathcal{SV}} = \mathrm{T}_k^{\gamma}\mathrm{T}_w^{\gamma}(id_{\mathcal{V}})$
$\mathcal{D}_{\mathcal{U}} = \mathcal{D}_{\kappa_{\mathcal{SU}}}(\mathcal{C}_{\mathcal{U}}) = \{id_{\mathcal{U}} \parallel id_{\mathcal{V}} \parallel \mathrm{H}_{\mathcal{U}} \parallel \mathrm{T}_r^{\gamma}(id_{\mathcal{V}})\}$
$\mathcal{D}_{\mathcal{V}} = \mathcal{D}_{\kappa_{\mathcal{SV}}}(\mathcal{C}_{\mathcal{V}}) = \{id_{\mathcal{V}} \parallel \mathrm{H}_{\mathcal{V}} \parallel \mathrm{T}_w^{\gamma}(id_{\mathcal{V}})\}$
Check $id_{\mathcal{U}}, id_{\mathcal{V}}$
Check $\mathrm{H}_{\mathcal{U}} =? \hbar(\mathrm{T}_r^{\gamma}(id_{\mathcal{U}}) \parallel id_{\mathcal{U}} \parallel id_{\mathcal{V}})$
$\mathrm{H}_{\mathcal{V}} =? \hbar(\mathrm{T}_w^{\gamma}(id_{\mathcal{V}}) \parallel id_{\mathcal{V}})$
$\mathrm{H}_{\mathcal{SU}} = \hbar(\mathrm{T}_k^{\gamma}(id_{\mathcal{U}}) \parallel \mathrm{T}_r^{\gamma}(id_{\mathcal{U}}))$
$\mathrm{H}_{\mathcal{SV}} = \hbar(\mathrm{T}_k^{\gamma}(id_{\mathcal{V}}) \parallel \mathrm{T}_w^{\gamma}(id_{\mathcal{V}}))$
$\mathcal{C}'_{\mathcal{U}} = \mathcal{E}_{\kappa_{\mathcal{SU}}}(id_{\mathcal{U}} \parallel id_{\mathcal{V}} \parallel \mathrm{T}_w^{\gamma}(id_{\mathcal{V}}) \parallel \mathrm{H}_{\mathcal{SU}})$
$\mathcal{C}'_{\mathcal{V}} = \mathcal{E}_{\kappa_{\mathcal{SV}}}(id_{\mathcal{U}} \parallel id_{\mathcal{V}} \parallel \mathrm{T}_r^{\gamma}(id_{\mathcal{V}}) \parallel \mathrm{H}_{\mathcal{SV}})$
$C'_{\mathcal{U}}, C'_{\mathcal{V}}$
Decrypt $\mathcal{C}'_{\mathcal{V}}$
Check $\mathrm{H}_{\mathcal{SV}}$ and $id_{\mathcal{U}}$
$\mathcal{S}\kappa = \mathrm{T}_w^{\gamma}\mathrm{T}_r^{\gamma}(id_{\mathcal{V}})$
$\mathrm{H}_{\mathcal{VU}} = \hbar(\mathcal{S}\kappa \parallel \mathcal{C}'_{\mathcal{U}})$
$\mathcal{C}'_{\mathcal{U}}, \mathrm{H}_{\mathcal{VU}}$
Decrypt $\mathcal{C}'_{\mathcal{U}}$
Check $\mathrm{H}_{\mathcal{SU}}$
$\mathcal{S}\kappa = \mathrm{T}_r^{\gamma}\mathrm{T}_w^{\gamma}(id_{\mathcal{V}})$
Check $\mathrm{H}_{\mathcal{VU}}$
$\mathrm{H}_{\mathcal{UV}} = \hbar(\mathcal{S}\kappa \parallel id_{\mathcal{U}} \parallel \mathrm{T}_r^{\gamma}(id_{\mathcal{V}}))$
$\mathrm{H}_{\mathcal{UV}}$
Check $\mathrm{H}_{\mathcal{UV}}$
Session key $\mathcal{S}\kappa' = \hbar(\mathcal{S}\kappa)$

Figure 2: Our proposed framework

5 The Formal Authentication Proof Using BAN Logic

The BAN logic is a well-known method of ensuring that information exchange protocols are valid. In this section, we will examine the accuracy of the session key among $\mathcal{U}$ and $\mathcal{V}$ using BAN logic [35,36]. To begin, the following are the notations, goals, and assumptions:

5.1 Notations

The notations and syntax of the BAN logic are defined here. The specific participants are defined as $\mathcal{U}$ and $\mathcal{V}$, the trusted server is $\mathcal{S}$, and the formula is $\mathcal{X}$ (statement). The following are some guidelines [1,17]:

1. $\mathcal{U}| \equiv \mathcal{X}$ means $\mathcal{U}$ trusts the formulation $\mathcal{X}$ is true.
2. $\mathcal{U}|\equiv \mathcal{V}$ means $\mathcal{U}$ trusts $\mathcal{V}$'s act.
3. $\mathcal{U} \triangleleft \mathcal{X}$ means $\mathcal{U}$ holds or sees the formulation $\mathcal{X}$.
4. $\mathcal{U}| \sim \mathcal{X}$ means $\mathcal{U}$ has said the formulation $\mathcal{X}$.
5. $\mathcal{U}| \Rightarrow \mathcal{X}$ means $\mathcal{U}$ has comprehensive control over the formulation $\mathcal{X}$.
6. $\overset{\kappa_{\mathcal{U}}}{\rightarrow}$ $\mathcal{U}$ means κ is the public key for $\mathcal{U}$ and $\kappa_{\mathcal{U}}^{-1}$ is the private key for $\mathcal{U}$.
7. $\frac{\mathit{Rule\ 1}}{\mathit{Rule\ 2}}$ means *Rule* 2 is from *Rule* 1.
8. $\mathcal{U} \overset{x}{\leftrightarrow} \mathcal{V}$ means x is a secret key, or secret info shared among $\mathcal{U}$ and $\mathcal{V}$.
9. $\{\mathcal{X}\}_{\kappa}$ means $\mathcal{X}$ is encrypted by the key κ.

5.2 Goals

In our system, there are three roles: $\mathcal{U}$ and $\mathcal{V}$ are the users who must use the trusted server ($\mathcal{S}$) to generate a common session key between them.

In the language of BAN logic, our strategy aims to achieve four objectives:

G1. $\mathcal{V}| \equiv \mathcal{S}| \equiv \mathcal{U} \triangleleft\ \mathrm{T}_k^{\gamma}(id_{\mathcal{U}})$
G2. $\mathcal{U}| \equiv \mathcal{S}| \equiv \mathcal{V} \triangleleft\ \mathrm{T}_k^{\gamma}(id_{\mathcal{V}})$
G3. $\mathcal{U}| \equiv \mathcal{V} \triangleleft \mathcal{U} \overset{\mathcal{S}\kappa}{\leftrightarrow} \mathcal{V}$
G4. $\mathcal{V}| \equiv \mathcal{U} \triangleleft \mathcal{U} \overset{\mathcal{S}\kappa}{\leftrightarrow} \mathcal{V}$

Because $\mathcal{U}$ and $\mathcal{V}$ must generate a shared session key to communicate, $\mathcal{U}$ must believe that the server believes $\mathcal{V}$ and that $\mathcal{V}$ possesses the session key $\mathcal{S}\kappa$, and vice versa.

5.3 Suppositions

The assumptions must be presented once the goals have been established:

$S1 \cdot \mathcal{U} \triangleleft id_{\mathcal{U}}$

$S2 \cdot \mathcal{U} \triangleleft id_{\mathcal{V}}$

$S3 \cdot \mathcal{V} \triangleleft id_{\mathcal{V}}$

$S4 \cdot \mathcal{U}| \Rightarrow r$

$S5 \cdot \mathcal{V}| \Rightarrow w$

$S6 \cdot \mathcal{S}| \Rightarrow (\mathrm{T}_k^{\gamma}(id_{\mathcal{U}}), T_{\kappa}^{\gamma}(id_{\mathcal{V}}))$

$\mathcal{U}$ and $\mathcal{V}$ each have their own identities in assumptions S1 through S3. Because $\mathcal{U}$ desires to create a common session key with $\mathcal{V}$, $\mathcal{U}$ must first possess the identity of $\mathcal{V}$, so that the server $\mathcal{S}$ can verify the identities of both parties in this connection. In suppositions S4 through S6, $\mathcal{U}$, $\mathcal{V}$ and $\mathcal{S}$ must each choose their private keys, which they control entirely.

5.4 Verification

We will use the BAN logic to check the accuracy of our suggested framework in this part. The main steps in the evidence are as follows:

$\mathcal{U}$ calculates $\kappa_{\mathcal{US}}$ and $\mathtt{H}_{\mathcal{U}}$

Message 1: $\mathcal{U} \rightarrow \mathcal{V}: (\mathtt{M}_1 = \mathtt{T}_r^{\gamma}(id_{\mathcal{U}}),\ \{id_{\mathcal{U}} \parallel id_{\mathcal{V}} \parallel \mathtt{H}_{\mathcal{U}} \parallel \mathtt{T}_r^{\gamma}(id_{\mathcal{V}})\}_{\kappa_{\mathcal{US}}})$

$V1. \mathcal{V} \lhd \mathtt{M}_1$

$\mathcal{V}$ calculates $\kappa_{\mathcal{US}}$ and $\mathtt{H}_{\mathcal{V}}$

Message 2: $\mathcal{V} \rightarrow \mathcal{S}: (\mathtt{M}_1,\ \mathtt{M}_2 = \mathtt{T}_w^{\gamma}(id_{\mathcal{V}}),\ \{id_{\mathcal{V}} \parallel \mathtt{H}_{\mathcal{V}} \parallel \mathtt{T}_w^{\gamma}(id_{\mathcal{V}})\}_{\kappa_{\mathcal{VS}}})$

$V2. \mathcal{S} \lhd \mathtt{M}_1,\ \mathtt{M}_2$

$\mathcal{S}$ calculates $\kappa_{\mathcal{SU}}, \kappa_{\mathcal{SV}}$

$$V3. \frac{\mathcal{S} \lhd \kappa_{\mathcal{SU}},\ \ \kappa_{\mathcal{SV}}}{\mathcal{S} \lhd id_{\mathcal{U}},\ id_{\mathcal{V}},\ \mathtt{H}_{\mathcal{U}},\ \mathtt{H}_{\mathcal{V}},\ T_r^{\gamma}(id_{\mathcal{U}}),\ \mathtt{T}_w^{\gamma}(id_{\mathcal{V}})}$$

$$V4. \frac{\mathcal{S} \lhd id_{\mathcal{U}},\ id_{\mathcal{V}},\ \mathtt{H}_{\mathcal{U}},\ \mathtt{H}_{\mathcal{V}},\ \mathtt{T}_r^{\gamma}(id_{\mathcal{U}}),\ T_w^{\gamma}(id_{\mathcal{V}}),\ \mathcal{S}| \Rightarrow (\mathtt{T}_k^{\gamma}(id_{\mathcal{U}}), \mathtt{T}_{\kappa}^{\gamma}(id_{\mathcal{V}}))}{\mathcal{S}| \equiv \kappa_{\mathcal{SU}},\ \kappa_{\mathcal{SV}}}$$

$$V5. \frac{\mathcal{S}| \equiv \kappa_{\mathcal{SU}},\ \kappa_{\mathcal{SV}}, \mathcal{S}| \Rightarrow (\mathtt{T}_k^{\gamma}(id_{\mathcal{U}}), \mathtt{T}_{\kappa}^{\gamma}(id_{\mathcal{V}}))}{\mathcal{S}| \equiv \mathcal{U} \lhd\ \mathtt{T}_k^{\gamma}(id_{\mathcal{U}}), \mathcal{S}| \equiv \mathcal{V} \lhd\ \mathtt{T}_k^{\gamma}(id_{\mathcal{V}})}$$

$\mathcal{S}$ calculates $H_{\mathcal{SU}}, \mathtt{H}_{\mathcal{SV}}$

Message 3: $\mathcal{S} \rightarrow \mathcal{V}: (\{id_{\mathcal{U}} \parallel id_{\mathcal{V}} \parallel \mathtt{T}_w^{\gamma}(id_{\mathcal{V}}) \parallel \mathtt{H}_{\mathcal{SU}}\}_{\kappa_{\mathcal{SU}}},\ \{id_{\mathcal{U}} \parallel id_{\mathcal{V}} \parallel \mathtt{T}_r^{\gamma}(id_{\mathcal{V}}) \parallel \mathtt{H}_{\mathcal{SV}}\}_{\kappa_{\mathcal{SV}}})$

$V6. \mathcal{V} \lhd \{id_{\mathcal{U}} \parallel id_{\mathcal{V}} \parallel \mathtt{T}_w^{\gamma}(id_{\mathcal{V}}) \parallel \mathtt{H}_{\mathcal{SU}}\}_{\kappa_{\mathcal{SU}}},\ \{id_{\mathcal{U}} \parallel id_{\mathcal{V}} \parallel \mathtt{T}_r^{\gamma}(id_{\mathcal{V}}) \parallel \mathtt{H}_{\mathcal{SV}}\}_{\kappa_{\mathcal{SV}}}$

$$V7. \frac{\mathcal{V} \lhd \kappa_{\mathcal{VS}}}{\mathcal{V} \lhd id_{\mathcal{U}},\ \mathtt{T}_r^{\gamma}(id_{\mathcal{V}}),\ \mathtt{H}_{\mathcal{SV}}}$$

$$V8. \frac{\mathcal{V} \lhd \mathtt{T}_k^{\gamma}(id_{\mathcal{V}})}{\mathcal{V}| \equiv \mathcal{S}| \sim \mathtt{H}_{\mathcal{SV}}}$$

$$V9. \frac{\mathcal{V}| \equiv \mathcal{S}| \sim \mathtt{H}_{\mathcal{SV}}}{\mathcal{V}| \equiv \mathcal{S}| \equiv \mathcal{U} \lhd\ \mathtt{T}_k^{\gamma}(id_{\mathcal{U}}), \mathcal{V}| \equiv \mathtt{T}_r^{\gamma}(id_{\mathcal{V}})}$$

$\mathcal{V}$ calculates $\mathcal{U} \overset{\mathcal{S}\kappa}{\leftrightarrow} \mathcal{V}, \mathtt{H}_{\mathcal{VU}}$

Message 4: $\mathcal{V} \rightarrow \mathcal{U} : \{id_{\mathcal{U}} \parallel id_{\mathcal{V}} \parallel \mathtt{T}_w^{\gamma}(id_{\mathcal{V}}) \parallel \mathtt{H}_{\mathcal{SU}}\}_{\kappa_{\mathcal{SU}}},\ \mathtt{H}_{\mathcal{VU}}$

$V10. \mathcal{U} \lhd \{id_{\mathcal{U}} \parallel id_{\mathcal{V}} \parallel \mathtt{T}_w^{\gamma}(id_{\mathcal{V}}) \parallel \mathtt{H}_{\mathcal{SU}}\}_{\kappa_{\mathcal{SU}}},\ \mathtt{H}_{\mathcal{VU}}$

$$V11.\ \frac{\mathcal{U} \lhd \kappa_{\mathcal{US}}}{\mathcal{U} \lhd \text{Ƭ}_{w}^{\gamma}(\imath d_{\mathcal{V}}),\ \text{Ҥ}_{\mathcal{SU}}}$$

$$V12.\ \frac{\mathcal{U} \lhd \text{Ƭ}_{k}^{\gamma}(\imath d_{\mathcal{U}})}{\mathcal{U}| \equiv \mathcal{S}| \sim \text{Ҥ}_{\mathcal{SU}}}$$

$$V13.\ \frac{\mathcal{U}| \equiv \mathcal{S}| \sim \text{Ҥ}_{\mathcal{SU}}}{\mathcal{U}| \equiv \mathcal{S}| \equiv \mathcal{V} \lhd\ \text{Ƭ}_{k}^{\gamma}(\imath d_{\mathcal{V}}),\ \ \mathcal{U}| \equiv \text{Ƭ}_{w}^{\gamma}(\imath d_{\mathcal{V}})}$$

$$V14. \frac{\mathcal{U}| \Rightarrow r, \mathcal{U}| \equiv \text{Ƭ}_{w}^{\gamma}(\imath d_{\mathcal{V}})}{\mathcal{U}| \equiv \text{Ҥ}_{\mathcal{VU}}}$$

$$V15.\ \frac{\mathcal{U}| \equiv \text{Ҥ}_{\mathcal{VU}}}{\mathcal{U}| \equiv \mathcal{V} \lhd \mathcal{U} \overset{\mathcal{S}\kappa}{\leftrightarrow} \mathcal{V}}$$

$\mathcal{U}$ calculates $\text{Ҥ}_{\mathcal{UV}}$

Message 5: $\mathcal{U} \rightarrow \mathcal{V} : \text{Ҥ}_{\mathcal{UV}}$

$$V16.\ \frac{\mathcal{V}| \equiv \mathcal{U} \overset{\mathcal{S}\kappa}{\leftrightarrow} \mathcal{V}, T_{r}^{\gamma}(\imath d_{\mathcal{V}})}{\mathcal{V}| \equiv \text{Ҥ}_{\mathcal{UV}}}$$

$$V17.\ \frac{\mathcal{V}| \equiv \text{Ҥ}_{\mathcal{UV}}}{\mathcal{V}| \equiv \mathcal{U} \lhd \mathcal{U} \overset{\mathcal{S}\kappa}{\leftrightarrow} \mathcal{V}}$$

$\mathcal{V}$ and $\mathcal{U}$ believe the server has said $\text{Ҥ}_{\mathcal{SV}}$ and $\text{Ҥ}_{\mathcal{SU}}$ in formulation V9 and formula V13. Because the server must check the certificate before giving $\text{Ҥ}_{\mathcal{SV}}$ and $\text{Ҥ}_{\mathcal{SU}}$, both $\mathcal{U}$ and $\mathcal{V}$ assume the other is an authorized user. Because $\mathcal{U}$ has r, $\text{Ƭ}_{w}^{\gamma}(\imath d_{\mathcal{V}})$, in formula V15, $\mathcal{U}$ may compute the session key $\mathcal{S}\kappa$. When $\mathcal{U}$ can decode $C'_{\mathcal{U}}$ and has $\mathcal{S}\kappa$, $\mathcal{U}$ can believe $\text{Ҥ}_{\mathcal{VU}}$, which leads $\mathcal{U}$ to believe that $\mathcal{V}$ has the secret value $\mathcal{S}\kappa$. Similarly, $\mathcal{V}$ believes that $\mathcal{U}$ possesses the secret value $\mathcal{S}\kappa$ in formulation V17. $\mathcal{U}$ and $\mathcal{V}$ can generate a common session key using this secret value. We may deduce that our approach accomplishes the goals using formulas V9, V13, V15, and V17.

6 Security Analysis and Discussions

This section provides a check to confirm that the presented technique supports mutual authentication, perfect forward secrecy, and user anonymity. Additionally, we put the suggested technique to the test against several attacks, including the man-in-the-middle attack, privileged insider attack, known-key secrecy, perfect forward secrecy, password guessing attacks, Clock synchronization problem, and the user identity forgery.

Hypothesis 1: The proposed technique can successfully resist the man-in-the-middle attack.

Justification: The attacker cannot manufacture a valid message using the suggested technique since the attacker does not have access to the secret values $\text{Ƭ}_{r}^{\gamma}(\imath d_{\mathcal{U}})$ and $\text{Ƭ}_{w}^{\gamma}(\imath d_{\mathcal{V}})$, which are used to generate the hash values $\text{Ҥ}_{\mathcal{U}}$ and $\text{Ҥ}_{\mathcal{V}}$. Furthermore, by checking hash values, both users ($\mathcal{U}$ and $\mathcal{V}$) and the server might determine whether the received messages were edited or substituted. The server examines $\text{Ҥ}_{\mathcal{U}}$ and $\text{Ҥ}_{\mathcal{V}}$ in step 3. The user $\mathcal{V}$ checks $\text{Ҥ}_{\mathcal{SV}}$ and $\text{Ҥ}_{\mathcal{VU}}$ in steps (4) and (6), while the user $\mathcal{U}$ checks $\text{Ҥ}_{\mathcal{SU}}$ and $\text{Ҥ}_{\mathcal{VU}}$ in step (5). As a result, the proposed technique can successfully defend against a man-in-the-middle attack.

Hypothesis 2: The proposed technique can offer mutual authentication among the users $\mathcal{U}$, $\mathcal{V}$ and the server $\mathcal{S}$.

Justification: Mutual authentication is a critical aspect of user authentication techniques since it allows any scheme member to authenticate the others. By computing secret keys $\kappa_{\mathcal{SU}}$ and $\kappa_{\mathcal{SV}}$, the server $\mathcal{S}$ can extract $id_{\mathcal{U}}$ and $id_{\mathcal{V}}$ from $\mathtt{M}_1$ and $id_{\mathcal{V}}$ from $\mathtt{M}_2$ using the proposed technique. The hash values $\mathrm{H}'_{\mathcal{V}}$ and $\mathrm{H}'_{\mathcal{U}}$ can then be computed. The server $\mathcal{S}$ can authenticate both users by checking whether $\mathrm{H}'_{\mathcal{U}} = \mathrm{H}_{\mathcal{U}}$ and $\mathrm{H}'_{\mathcal{V}} = \mathrm{H}_{\mathcal{V}}$ are equal. The user $\mathcal{U}$ can compute $\mathrm{H}'_{\mathcal{SU}}$ and authenticate the server $\mathcal{S}$ by checking if $\mathrm{H}'_{\mathcal{SU}} = \mathrm{H}_{\mathcal{SU}}$ in step (5). She/he can also verify the identity of user $\mathcal{V}$ by looking at the received value $\mathrm{H}_{\mathcal{VU}}$. The user $\mathcal{V}$ can calculate $\mathrm{H}_{\mathcal{SV}}$ and verify if $\mathrm{H}'_{\mathcal{SV}} = \mathrm{H}_{\mathcal{SV}}$ to authenticate the server. $\mathcal{V}$ authenticates the user $\mathcal{U}$ in step (6) by checking the received value $\mathrm{H}_{\mathcal{VU}}$. As a result, all parties can establish mutual authentication using the proposed technique.

Hypothesis 3: The proposed technique protects the user's anonymity.

Justification: When the two users create their shared session key, they must inform each other and the server $\mathcal{S}$ of their identities. In other words, the sender's identity is included in the message transmitted from one user to another. In our technique, the identity in the message sent during communication is encrypted using fractional chaotic maps rather than plaintext. If a malicious attacker intercepts the communication, the attacker will be unable to deduce the user's true identity by examining the message.

Hypothesis 4: The proposed technique protects against user identity forgery.

Justification: The identities of the two users are included in the message sent to server $\mathcal{S}$. (one encrypted by using the fractional chaotic maps and the other not). When the server $\mathcal{S}$ receives the communication, it can quickly decrypt it and verify the identities of both users.

Hypothesis 5: The proposed technique need not require a password table.

Justification: A password table must exist on the server-side for a password authentication technique to effectively save and update the legal participants' passwords. An insider attack could occur if the server has malicious intentions, and passwords could be exploited or manipulated. There is no password table on the server-side of our technique because we do not maintain the participants' passwords. Hence there is no possibility of an insider attack.

Hypothesis 6: The proposed technique is secured against password guessing attacks.

Justification: A password authentication mechanism will always be vulnerable to a password guessing attack. After intercepting a transmission, the attacker will guess the proper password. If the password is accurately guessed, the attacker can use it to commit fraud. Unlike password authentication techniques, our technique does not rely on passwords, it is immune to password guessing attacks.

Hypothesis 7: The proposed technique is secured against the Clock synchronization problem.

Justification: Unlike many previous key agreement techniques, the proposed key agreement technique could continue to work even if the clock is out of sync, ensuring secure communication between sender and receiver. Because the timestamp is merely relative to the receiver's clock, synchronized clocks are unnecessary. The timestamp generated by the receiver is the only one he verifies.

Hypothesis 8: The proposed technique can offer known-key secrecy.

Justification: Even if the sender intercepts the prior session keys, our presented technique can offer known-key secrecy because the next session keys cannot be exposed. If a sender intercepts a session key $\mathcal{S}\kappa = \mathtt{T}^{\gamma}_{w}\mathtt{T}^{\gamma}_{r}(id_{\mathcal{V}})$ and knows the random parameters w and r, she will be unable to obtain the preceding and subsequent session keys due to the unknown random parameters.

Hypothesis 9: The proposed technique can offer perfect forward secrecy.

Justification: Creating a session key among communication entities is independent of previously generated session keys. Our presented technique can ensure perfect forward secrecy. Even though the sender can intercept the parameters $\mathrm{T}^{\gamma}_{r}(id_{v})$ and $\mathrm{T}^{\gamma}_{w}(id_{v})$, which are typically transmitted over a channel, they are unable to compute the following session key $\mathcal{S}\kappa = \mathrm{T}^{\gamma}_{w}\mathrm{T}^{\gamma}_{r}(id_{v})$ due to the intractability of the fractional chaotic maps-based Diffie-Hellman (FCMDH) and fractional chaotic maps-based Discrete Logarithm (FCMDL) problems, and Alice hasn't been able to get the following session key before.

7 Performance Comparisons

We demonstrate the efficiency of the presented technique in this portion of the article. Tab. 3 compares the security features of our suggested technique to those of Lee et al. [37], Zhao et al. [38], Farash et al. [39], Xie et al. [40], and Jabbari et al. [41] techniques. Under key considerations, our proposed technique provides higher security than the other techniques. In addition, we compared the computational primitives employed in our proposed technique's positioning of the users and server to those used in other relevant techniques.

Table 3: Security characteristics comparisons between the provided and other similar techniques

Techniques → Security Attributes↓	[37]	[38]	[39]	[40]	[41]	Proposed Technique
$\mathcal{SA}1$	N	***Y***	N	***Y***	***Y***	***Y***
$\mathcal{SA}2$	N	***Y***	N	N	***Y***	***Y***
$\mathcal{SA}3$	***Y***	***Y***	N	N	***Y***	***Y***
$\mathcal{SA}4$	***Y***	N	N	***Y***	N	***Y***
$\mathcal{SA}5$	***Y***	N	***Y***	N	***Y***	***Y***
$\mathcal{SA}6$	***Y***	***Y***	N	***Y***	N	***Y***
$\mathcal{SA}7$	N	N	N	N	N	***Y***
$\mathcal{SA}8$	N	N	N	***Y***	***Y***	***Y***
$\mathcal{SA}9$	N	N	N	***Y***	N	***Y***

Note: $\mathcal{SA}1$*: man-in-the-middle attack;* $\mathcal{SA}2$*: mutual authentication;* $\mathcal{SA}3$*: user anonymity;* $\mathcal{SA}4$*: user identity forgery;* $\mathcal{SA}5$*: required a password table;* $\mathcal{SA}6$*: password guessing attacks;* $\mathcal{SA}7$*: Clock synchronization problem;* $\mathcal{SA}8$*: known-key secrecy;* $\mathcal{SA}9$*:perfect forward secrecy. Note:* ***Y****: Secure;* N*: Vulnerable.*

In this contrast study, we employed the four-time complexity notations listed below.:t_{h}, t_{ch} ,t_{s}, and t_{m}described performance time for a one-way hash function, a Chebyshev chaotic map operation, a symmetric encryption/decryption operation, and one modular multiplication, respectively. The relations between: t_{ch}, t_{h}, t_{s}, and t_{m} with respect to $t_{h}(t_{h} = 0.32\ ms)$ have been known in several works [3,9,33], and $\gamma = 1/2$ since $\gamma \in [0, 1]$ [33]). The relationship and order of computational complexity between the metrics are as follows: $t_{s} \approx t_{h}$, $t_{\mathrm{ch}} \approx t_{\mathrm{h}}, t_{m} \approx 2.5\ t_{\mathrm{h}}$, and $t_{ch} \approx t_{\mathrm{h}} \approx t_{\mathrm{s}} < t_{m}$. Tab. 4 shows the performance evaluation of the proposed technique and the existing techniques' primary consuming techniques. Fig. 3 also displays millisecond (ms) comparisons of overall processing costs.

Table 4: Performance evaluation of the proposed scheme and other relevant techniques

Techniques	User ($\mathcal{U}$)	Server ($\mathcal{S}$)	User ($\mathcal{V}$)	Total
Lee et al. [37]	$4\mathfrak{t}_h + 4\mathfrak{t}_{ch} + 2\mathfrak{t}_s$	$4\mathfrak{t}_h + 4\mathfrak{t}_{ch} + 4\mathfrak{t}_s$	$4\mathfrak{t}_h + 3\mathfrak{t}_{ch} + 2\mathfrak{t}_s$	$12\mathfrak{t}_h + 11\mathfrak{t}_{ch} + 8\mathfrak{t}_s$
Zhao et al. [38]	$6\mathfrak{t}_h + 3\mathfrak{t}_{ch} + 1\mathfrak{t}_s$	$8\mathfrak{t}_h + 2\mathfrak{t}_{ch} + 2\mathfrak{t}_s$	$6\mathfrak{t}_h + 3\mathfrak{t}_{ch} + 1\mathfrak{t}_s$	$20\mathfrak{t}_h + 8\mathfrak{t}_{ch} + 4\mathfrak{t}_s$
Farash and Attari [39]	$4\mathfrak{t}_h + 3\mathfrak{t}_{ch}$	$4\mathfrak{t}_h + 2\mathfrak{t}_{ch} + 2\mathfrak{t}_m$	$4\mathfrak{t}_h + 3\mathfrak{t}_{ch}$	$12\mathfrak{t}_h + 8\mathfrak{t}_{ch} + 2\mathfrak{t}_m$
Xie et al. [40]	$4\mathfrak{t}_h + 3\mathfrak{t}_{ch} + 2\mathfrak{t}_s$	$4\mathfrak{t}_h + 2\mathfrak{t}_{ch} + 4\mathfrak{t}_s + 2\mathfrak{t}_m$	$4\mathfrak{t}_h + 3\mathfrak{t}_{ch} + 2\mathfrak{t}_s$	$12\mathfrak{t}_h + 8\mathfrak{t}_{ch} + 8\mathfrak{t}_s + 2\mathfrak{t}_m$
Jabbari and Mohasefi [41]	$4\mathfrak{t}_h + 4\mathfrak{t}_{ch} + 2\mathfrak{t}_s$	$4\mathfrak{t}_h + 4\mathfrak{t}_{ch} + 4\mathfrak{t}_s$	$4\mathfrak{t}_h + 3\mathfrak{t}_{ch} + 2\mathfrak{t}_s$	$12\mathfrak{t}_h + 11\mathfrak{t}_{ch} + 8\mathfrak{t}_s$
Proposed Technique	$4\mathfrak{t}_h + 3\mathfrak{t}_{ch} + 2\mathfrak{t}_s$	$4\mathfrak{t}_h + 3\mathfrak{t}_{ch} + 4\mathfrak{t}_s$	$4\mathfrak{t}_h + 2\mathfrak{t}_{ch} + 2\mathfrak{t}_s$	$12\mathfrak{t}_h + 8\mathfrak{t}_{ch} + 8\mathfrak{t}_s$

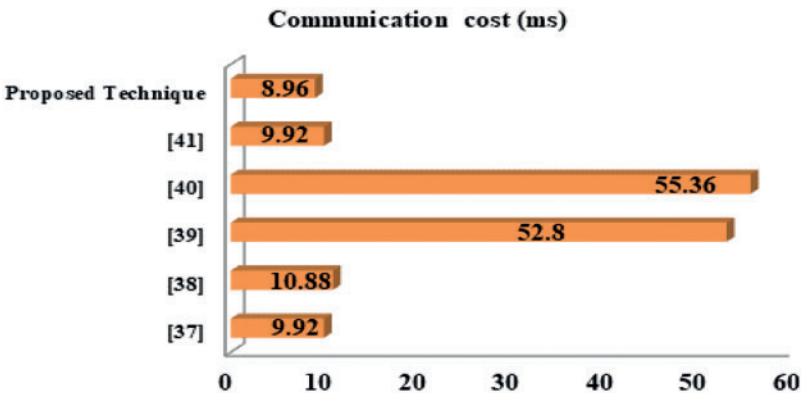

Figure 3: Total communication cost (ms)

On the other hand, our proposed technique can provide comprehensive security assurance at a cheap computing cost while displaying very high-efficiency thanks to Chebyshev chaotic maps and hash functions.

8 Conclusion

This paper proposed an efficient three-factor authenticated key agreement technique using fractional chaotic maps under the HC-IoT architecture without a password table. Our novel technique is entirely immune to password guessing attacks. Furthermore, our technique ensures that users' privacy is fully protected, ensuring that a user forging attack has no adverse consequences. Our novel strategy outperforms the currently available technique in terms of security. Also, we performed a BAN logic test and confirmed the correctness of our technique. However, the current paper has not deployed the experimental setting for the proposed scheme. In future work, we would focus on a lightweight three-factor authentication and key agreement technique for IoT multi-gateway wireless sensor networks leveraging extended Chebyshev chaotic maps.

Acknowledgement: The authors extend their gratitude to the Deanship of Scientific Research at King Khalid University for funding this work through the research group program under grant number R. G. P. 1/72/42. 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.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] J. Singh, A. Gimekar and S. Venkatesan, "An efficient lightweight authentication scheme for human-centered industrial internet of things," *International Journal of Communication Systems*, no. e4189, pp. 1–13, 2019.

[2] M. Saqib, B. Jasra and A. H. Moon, "A lightweight three factor authentication framework for IoT based critical applications," *Journal of King Saud University-Computer and Information Sciences*, pp. 1–13, 2021.

[3] C. Meshram, A. Alsanad, J. V. Tembhurne, S. W. Shende, K. W. Kalare *et al.,* "A provably secure lightweight subtree-based short signature scheme with fuzzy user data sharing for human-centered IoT," *IEEE Access*, vol. 9, pp. 3649–3659, 2021.

[4] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah *et al.,* "A robust ECC-based provable secure authentication protocol with privacy preserving for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3599–3609, 2018.

[5] J. Shen, S. Chang, J. Shen, Q. Liu and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," *Future Generation Computer Systems*, vol. 78, pp. 956–963, 2018.

[6] A. K. Das, M. Wazid, A. R. Yannam, J. J. P. C. Rodrigues and Y. Park, "Provably secure ECC-based device access control and key agreement protocol for IoT environment," *IEEE Access*, vol. 7, pp. 55382–55397, 2019.

[7] B. Ying and A. Nayak, "Anonymous and lightweight authentication for secure vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 12, pp. 10626–10636, 2017.

[8] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos and J. J. P. C. Rodrigues, "Design and analysis of secure lightweight remote user authentication and Key agreement scheme in internet of drones deployment," *IEEE Internet Things Journal*, vol. 6, no. 2, pp. 3572–3584, 2019.

[9] C. Meshram, M. S. Obaidat, J. V. Tembhurne, S. W. Shende, K. W. Kalare *et al.,* "A lightweight provably secure digital short-signature technique using extended chaotic maps for human-centered IoT systems," *IEEE Systems Journal*, vol. 15, no. 4, pp. 5507–5515, 2021.

[10] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1086–1090, 2009.

[11] J. Srinivas, S. Mukhopadhyay and D. Mishra, "Secure and efficient user authentication scheme for multi-gateway wireless sensor networks," *Ad Hoc Networks*, vol. 54, pp. 147–169, 2017.

[12] D. Wang, W. Li and P. Wang, "Measuring Two-factor authentication schemes for real-time data access in industrial wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4081–4092, 2018.

[13] A. Esfahani, G. Mantas, R. Matischek, F. B. Saghezchi, J. Rodriguez *et al.,* "A lightweight authentication mechanism for M2M communications in industrial IoT environment," *IEEE Internet Things Journal*, vol. 6, no. 1, pp. 288–296, 2019.

[14] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti *et al.,* "Design of secure user authenticated Key management protocol for generic IoT networks," *IEEE Internet Things Journal*, vol. 5, no. 1, pp. 269–282, 2018.

[15] M. S. Hossain and G. Muhammad, “Cloud-assisted industrial internet of things (IIoT) – enabled framework for health monitoring,” *Computer Networks*, vol. 101, pp. 192–202, 2016.

[16] X. Li, J. Peng, J. Niu, F. Wu, J. Liao *et al.,* “A robust and energy efficient authentication protocol for industrial internet of things,” *IEEE Internet Things Journal*, vol. 5, no. 3, pp. 1606–1615, 2018.

[17] Y. Yu, L. Hu and J. Chu, “A secure authentication and Key agreement scheme for IoT-based cloud computing environment,” *Symmetry*, vol. 12, no. 1, 150, pp. 1–16, 2020.

[18] H. Lee, D. Kang, Y. Lee and D. Won, “Secure three-factor anonymous user authentication scheme for cloud computing environment,” *Wireless Communication and Mobile Computing*, vol. 2021, pp. 2098530, 2021.

[19] A. S. Almogren, “Intrusion detection in edge-of-things computing,” *Journal of Parallel and Distributed Computing*, vol. 137, pp. 259–265, 2020.

[20] S. K. H. Islam, “Design of identity-based digital signature schemes using extended chaotic maps,” *IACR Cryptology ePrint Archive*, vol. 2014, pp. 275–280, 2014.

[21] G. Gao, X. Peng, Y. Tian and Z. Qin, “A chaotic maps-based authentication scheme for wireless body area networks,” *International Journal of Distributed Sensor Networks*, vol. 12, no. 7, pp. 2174720, 2016.

[22] Y. Lu, L. Li, H. Zhang and Y. Yang, “An extended chaotic maps-based three-party password- authenticated key agreement with user anonymity,” *PLoS One*, vol. 11, no. 4, pp. 1–19, 2016.

[23] C. Meshram, C.-C. Lee, S. G. Meshram and C.-T. Li, “An efficient ID-based cryptographic transformation model for extended chaotic-map-based cryptosystem,” *Soft Computing*, vol. 23, no. 16, pp. 6937–6946, 2019.

[24] L. Kocarev, “Chaos-based cryptography: A brief overview,” *IEEE Circuits Systems Magazine*, vol. 1, no. 3, pp. 6–21, 2001.

[25] P. Bergamo, P. Arco, A. Santis and L. Kocarev, “Security of public key cryptosystems based on chebyshev polynomials,” *IEEE Transactions on Circuits and Systems*, vol. 52, no. 7, pp. 1382–1393, 2005.

[26] L. Zhang, “Cryptanalysis of the public key encryption based on multiple chaotic systems,”, *Chaos Solitons & Fractals*, vol. 37, no. 3, pp. 669–674, 2008.

[27] C. Meshram, C. C. Lee, S. G. Meshram, C. T. Li, “An efficient ID-based cryptographic transformation model for extended chaotic-map-based cryptosystem,” *Soft Computing*, vol. 23, no. 16, pp. 6937–6946, 2019.

[28] C. Meshram, C. C. Lee, A. S. Ranadive, C. T. Li, S. G. Meshram *et al.,* “A subtree-based transformation model for cryptosystem using chaotic maps under cloud computing environment for fuzzy user data sharing,” *International Journal of Communication Systems*, vol. 33, no. 7, p. e4307, 2020.

[29] C. Meshram, C. C. Lee, S. G. Meshram and A. Meshram, “OOS-SSS: An efficient online/offline subtree-based short signature scheme using chebyshev chaotic maps for wireless sensor network,” *IEEE Access*, vol. 8, no. 1, pp. 80063–80073, 2020.

[30] C. Meshram, R. W. Ibrahim, L. Deng, S. W. Shende, S. G. Meshram *et al.,* “A robust smart card and remote user password-based authentication protocol using extended chaotic-maps under smart cities environment,” *Soft Computing*, vol. 25, no. 15, pp. 10037–10051, 2021.

[31] C. Meshram, M. S. Obaidat, J. V. Tembhurne, S. W. Shende, K. W. Kalare *et al.,* “A lightweight provably secure digital short signature technique using extended chaotic maps for human-centered IoT systems,” *IEEE Systems Journal*, vol. 15, no. 4, pp. 5507–5515, 2021.

[32] X. J. Yang, D. Baleanu and H. M. Srivastava, “Local fractional integral transforms and their applications,” *Elsevier/Academic Press, cop.*, 2016.

[33] C. Meshram, R. W. Ibrahim, A. J. Obaid, S. G. Meshram, A. Meshram *et al.,* “Fractional chaotic maps based short signature scheme under human-centredIoT environments,” *Journal of Advanced Research*, vol. 32, pp. 139–148, 2020.

[34] S. Han and E. Chang, “Chaotic map based key agreement with/out clock synchronization,” *Choas, Solitons and Fractals*, vol. 39, no. 3, pp. 1283–1289, 2009.

[35] M. Burrows, M. Abadi and R. Needham, “A logic of authentication,” *ACM Transactions Computer Systems*, vol. 8, no. 1, pp. 18–36, 1990.

[36] M. S. Farash and M. A. Attari, “An improved password-based authentication scheme for session initiation protocol using smart cards without verification table,” *International Journal of Communication Systems*, vol. 30, no. 1, pp. e2879, 2017.

[37] C. -C. Lee, C. -T. Li, S. -T. Chiu and Y. -M. Lai, “A new three party-authenticated key agreement scheme based on chaotic maps without password table,” *Nonlinear Dynamics*, vol. 79, no. 4, pp. 2485–2495, 2015.

[38] F. Zhao, P. Gong, S. Li, M. Li and P. Li, “Cryptanalysis and improvement of a three-party key agreement protocol using enhanced chebyshev polynomials,” *Nonlinear Dynamics*, vol. 74, no. 12, pp. 419–427, 2013.

[39] M. S. Farash and M. A. Attari, “An efficient and provably secure three-party password-based authenticated key exchange protocol based on chebyshev chaotic maps,” *Nonlinear Dynamics*, vol. 77, no. 12, pp. 399–411, 2014.

[40] Q. Xie, J. Zhao and X. Yu, “Chaotic maps-based three-party password-authenticated key agreement scheme,” *Nonlinear Dynamics*, vol. 74, no. 4, pp. 1021–1027, 2013.

[41] A. Jabbari and J. B Mohasefi,. “Improvement in new three-party-authenticated key agreement scheme based on chaotic maps without password table,” *Nonlinear Dynamics*, vol. 95, pp. 3177–3191, 2019.