The Journal of Supercomputing (2021) 77:8281–8304
https://doi.org/10.1007/s11227-020-03553-y

Provably secure lightweight client authentication scheme with anonymity for TMIS using chaotic hash function

Vishesh P. Gaikwad[1] · Jitendra V. Tembhurne[1] · Chandrashekhar Meshram[2] · Cheng-Chi Lee[3,4]

Accepted: 28 November 2020 / Published online: 19 January 2021

Abstract
Telecare medicine information system (TMIS) is recognized as an important tool for improving the quality and protection of healthcare services. In addition to protecting the privacy of patients, many authentication techniques are being introduced in TMIS. After investigations, it is observed that many authentication techniques have security breaches. In this article, we propose an efficient, secure and lightweight authentication scheme for TMIS using chaotic hash function to achieve user anonymity. Chaotic hash function constitutes potential security a set in modern cryptography with its random behavior. Also, we provide the security proof in the random oracle (RO) model and proof of correctness of algorithm is presented using (Burrows–Abadi–Needham) BAN logic for proposed scheme. The comprehensive formal and informal security review demonstrate that the security of our scheme is resistive against known potential attacks. Additionally, our presented authentication scheme performs significantly better as compared to other existing schemes in the literature and also it is efficient on the basis on high security and low cost for computational and communication.

Keywords Telecare medical information system · Authentication · Smart card · Password-based remote authentication · Chaotic hash function · Subtree · Fuzzy user · Random oracle

1 Introduction

With the advent of various computing resources and storage media, the large amount of data is generated by the different applications over the public communication network. Today, variety of data is available on our finger tips such as social media, stock market, finance, medical and healthcare, etc. All these data are very crucial and vital

✉ Cheng-Chi Lee
cclee@mail.fju.edu.tw

Extended author information available on the last page of the article

for any organization. Therefore, the challenge is to keep these data protected since the data movement is over the public network. In this article, we target the security and privacy of data generated by e-healthcare which is maintained on TMIS. The TMIS is designed to make it easier for patients to provide different healthcare services effortlessly. The main objective of TMIS is to store the medical data such as patient information, disease information, medical history and very important electronic medical records (EMRs) of patients, etc. This health information is vital to the patients, physicians, medical practitioner and hospitals. Using TMIS, patient at remote or distant location can post and get healthcare data or services over the public network. So, this system facilitates the patients in saving time and related expenses incurred in attaining the hospital physically. But, preserving patient's security and privacy over public network is the challenging task. Also, physicians or doctors can monitor the patients to investigate or suggest healthcare services on need or demand. Due to superior facilities in telecommunication, wireless and mobile communication enriches the quality services in medical domain. Thus, we need strong mechanism to prevent unauthorized access of data, protection against EMRs confidentiality, and better availability of medical system. The efficient authentication mechanism is desired to protect against integrity, security, and authenticity of data transmitted over public network for TMIS. Hence, the main objective of this work is to propose a secure authentication scheme to preserve the user anonymity over public communication channel for TMIS. Moreover, detailed security analysis and security proofs is investigated to verify the security of propose scheme for different types of attacks.

In the literature, various authentication schemes are presented to ensure integrity, security, authenticity, and confidentiality. The early smart card and password authentication scheme has several advantages, i.e., smart card design protects against tamper resistance which is demonstrated in [1–8]. An authentication scheme based on passwords for TMIS is presented [9] wherein the scheme is efficient because of avoiding costlier computation of exponentiation as well as protects against a variety of attacks includes; stolen-verifier, guessing off-line/on-line password attack, and replay attack, etc. Furthermore, an impersonation attack is identified in [9], to overcome this attack for mobile devices (low power) in TMIS environment is illustrated in [10]. In [11], an authentication technique using dynamic ID for TMIS is proposed which suffers from user anonymity and password stolen attacks. Thus, improved dynamic ID-based schemes are designed [12–14] which is prevailing the attacks in [11].

Lee et al. in 2013 presented a secure authentication scheme based on password for smart cards in integrated electronic patient record (EPR) system [15]. Later, [16, 17] identified the security breach in [15], i.e., replay attack, stolen verifier attack, stolen smart card attack, impersonation attack, and presented more secure authentication schemes to resolve all the issues in [15]. In 2014, He et al. [2] formulated new authentication technique based on elliptic curve cryptography (ECC) and RFID using ID verifier wherein it overcomes the drawbacks of previous schemes. Moreover, performance measures are analyzed based on storage needed, and computation and communication cost. Similarly, ECC-based RFID [18] authentication review is presented to analyze the security and performance in healthcare environment using Internet of Things (IoTs).

1.1 Contribution

From the above findings and investigation, we need a robust and secure authentication scheme for TMIS. Hence, we present the various targeted contributions in this article for the proposal of new authentication scheme. The contributions are listed as follows:

1. To propose an efficient scheme for lightweight and secure client authentication for TMIS using subtree under fuzzy user's data sharing environments with anonymity. The proposed scheme utilizes one-way chaotic hash function which is secure and collision-resistant, and bitwise XOR operation.
2. To present security proofs in RO model and proof of correctness using BAN logic.
3. Our new scheme is client-friendly, i.e., it provides the client with the power to directly modify/update their password and personal biometric key without contacting to base station.
4. To present thorough security examinations which includes: formal analysis and an informal investigation. Hence, the verification of proposed scheme is investigated for different attacks.

1.2 Road map of the article

In Sect. 2, we present the literature review related to authentication schemes in TMIS. In Sect. 3, we present the background material, concept of chaotic hash function, and attacker model. Section 4 demonstrates the complete details of proposed scheme for TMIS. The analysis of security for proposed scheme in TMIS is discussed in Sect. 5. Section 6 shows the performance comparison, and conclusions are highlighted in Sect. 7.

2 Related Works

Security and privacy of patient is the main concern in TMIS environment. To access healthcare services remotely, authentication of TMIS server and verification of patient is required. Lu et al. [19] presented a three-factor authentication method using biometric for TMIS, but after investigations it is found that the method is vulnerable to different attacks. In addition, patient untraceability is also not supported by the proposed method. In [20–22], vulnerabilities pointed in Lu et al. [19] are addressed and an improved biometric authentication schemes using ECC is implemented which is efficient against various attacks. Moreover, various techniques have been adopted in the literature to propose a robust and efficient authentication scheme that utilizes symmetric key [23], RSA [24], and key agreement [25] for TMIS.

Subsequently, numerous schemes were proposed to work against different attacks on TMIS. Maintaining the secrecy, authentication, and secure access to healthcare data is the challenging task in public network. A survey presented in [26] enriches to understand the applicability of authentication schemes toward security and

respective vulnerabilities against various attacks. The authentication is needed in various systems wherein important data are stored via public network. Hence, the two-factor authentication [27] method used for healthcare under wireless medical sensor networks, three-factor authentication [28] in smart city and multi-server setting [29], password-based [30] and certificateless aggregate signature [31] authentication for vehicular ad hoc network (VANET), end-to-end authentication [32] in wearable devices for monitoring health, key agreement [33] authentication in cloud for cyber-physical systems, and 3-factor authentication [34] for satellite communications were proposed.

In recent, secure and efficient authentication schemes are proposed to address the various attacks in TMIS. Wei et al. [35] highlighted that how 3-factor authentication preserves the privacy and maintain the security. In [36], another 3-factor authentication for preserving user anonymity using extended ECC is proposed; moreover, the verification of security for proposed scheme is presented using formal and informal ways. Authentication scheme using smart card to overcome an attack such as mutual authentication, user anonymity and secrecy is illustrated by Radhakrishnan et al. [37]. The authors fixed the shortcomings of Lee et al. [15] scheme for TMIS. Furthermore, an authentication based on TMIS developed in [38] is adopted to remove the drawbacks of [39], the vulnerabilities pointed to resolves are guessing password, server spoofing, and extraction of biometric parameter. Nevertheless, the more improved 3-factor authentication [40, 41] and authentication using key agreement [42, 43] are the major breakthrough witnessed in the field of TMIS authentication.

Most recently, in 2020, Dharminder et al. [44] proposed a RSA-based TMIS authentication scheme which targets to resolve the shortcomings of Radhakrishnan et al., and provide the generalized authentication scheme. Lastly, Lo et al. [45] performed the security analysis toward to facilitate the scheme to allow off-line password change. Herein, author has overcome the issues identified in [46].

The above literature review motivates to design new authentication scheme for TMIS to offer various security features. After investigating the existing schemes for TMIS, we found that the TMIS is vulnerable to different security attacks and health information can be stolen. So, to protect the health information from different attacks, we need secure and lightweight authentication scheme for TMIS. In this paper, we present a secure authentication scheme for subtree-based fuzzy user environment, adopting the concept of chaotic hash function to accomplish user anonymity.

3 Background material

In this section, we briefly familiarizes the notations used in our propose authentication scheme, attacker model and the basic concept of Chaotic hash function as well as some related mathematical points.

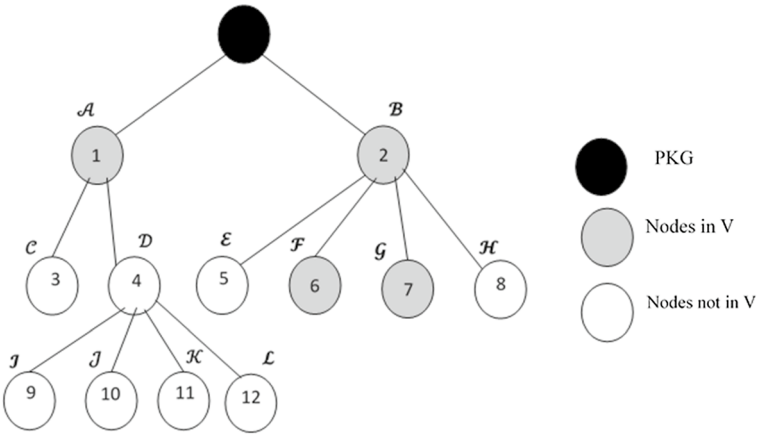

Fig. 1 Example of client authentication scheme

3.1 Notations

A client authentication scheme with anonymity for TMIS is a novel cryptographic primitive for fuzzy-entity data sharing. Let us see how some notations are defined, because these notations will be used in our new scheme.

For simplicity, we use $[x, y]$ for the shorthand of $\{x, x+1, \ldots, y\}$ and $[x]$ for $[1, x]$. For every $id = (id_1, id_2, \ldots, id_k)$, where id is an identity vector, let $S_{id} = \{id_1, \ldots, id_k\}$ is the set of (id). The id's location record in a tree is defined by $I_{id} = \{i; id_i \in S_{id}\}$. Identified receivers formulate a subtree which is related to tree-based encryption technique [47–50]. The id and respective places of receivers are joined into $\mathbb{T}$. The legitimate $\mathbb{T}$ must cover the root node. From this, we depict that the structure is managed by PKG. Similarly, identity set of $\mathbb{T}$ and location indices of $\mathbb{T}$ are expressed by $S_{\mathbb{T}} = \cup_{id \in \mathbb{T}} S_{id}$ and $I_{id} = \{i; id_i \in S_{\mathbb{T}}\}$, respectively. The symbolizations here can be expressed as $\mathrm{Sup}(id) = \{(id_1, id_2, \ldots, id_{k'}); k' \leq k\}$ to indicate the superiority of $id = (id_1, id_2, \ldots, id_k)$. Subtree, $\mathbb{T}$'s predictable receivers are categorized as $\mathrm{Sup}(\mathbb{T}) = \cup_{id \in \mathbb{T}} \mathrm{Sup}(id)$.

The presented symbolizations are found to be appropriate for proposed client authentication scheme based on subtree. Suppose that the users are structured as shown in Fig. 1 in a tree structure. The $S_{id} = \{\mathcal{B}, \mathcal{F}\}$ and $I_{id} = \{2, 6\}$ are used to specify a known user with $id = (\mathcal{B}, \mathcal{F})$. The $\mathrm{Sup}(id) = \{(\mathcal{B}), (\mathcal{B}, \mathcal{F})\}$, a set is created by the user involving superiors of him/her. When message is send by the data owner to the receivers set in a subtree, i.e., $\mathbb{T} = \{(\mathcal{A})(\mathcal{B}, \mathcal{F}), (\mathcal{B}, \mathcal{G})\}$, then $\mathbb{T}$'s identity set is denoted by $S_{\mathbb{T}} = \{\mathcal{A}, \mathcal{B}, \mathcal{F}, \mathcal{G}\}$, and $\mathbb{T}$'s position indices are represented by $I_{\mathbb{T}} = \{1, 2, 6, 7\}$, whereas superiors of $\mathbb{T}$'s are expressed by $\mathrm{Sup}(\mathbb{T}) = \{(\mathcal{A}), (\mathcal{B}), (\mathcal{B}, \mathcal{F}), (\mathcal{B}, \mathcal{G})\}$, we see user agreement toward data owner is conveyed.

3.2 Chaotic hash function

Chaotic hash function is a one-dimensional and piece-wise linear map [47–52], expressed as follows:

$$y_{i+1} = \begin{cases} \frac{y_i}{\gamma}, & \text{if} \quad 0 \le y_i < \gamma \\ \frac{y_i - \gamma}{0.5 - \gamma}, & \text{if} \quad \gamma \le y_i < 0.5 \\ \frac{1 - y_i - \gamma}{0.5 - \gamma}, & \text{if} \quad 0.5 \le y_i < 1 - \gamma \\ \frac{1 - y_i}{\gamma}, & \text{if} \quad 1 - \gamma \le y_i < 1 \end{cases}$$

where the control parameter are $y_i \in [0, 1]$ and $\gamma \in (0, 0.5)$. The parameter γ in y_{i+1} guarantees the operation of map under chaotic state on utilizing $0 < \gamma < 0.5$. The self-transformation of map is performed at $[0, 1]$, containing only a parameter γ. Chaining variables y_0 and y_i are used initially for the transformation, these chaining variables are the indicators in an algorithm for one-way hash.

3.3 Model for attacker

The insecure channel is chosen for the experimentation of authentication scheme proposed in this article. We assume following capabilities an adversary can hold. The valid assumptions are listed as follows:

1. An adversary can extract information from smart card by power consumption monitoring [53, 54], when smart card is lost or stolen.
2. Messages transmitted among the entities through public channel can be eavesdropped by an adversary.
3. Eavesdrop messages can be updated and resend, and reroute by an adversary (Table 1).

4 Proposed scheme

Here, we present an anonymity preserving efficient authentication scheme for TMIS. The scheme is protective against different security breaches, even though smart card is compromised. The identified phases of operations in the proposed scheme are similar to the related existing schemes, i.e., *registration phase*, *login phase*, *verification phase*, and *password change phase*. Detail description of proposed scheme is presented as follows and same is shown in Fig. 2.

Table 1 Notations

Notations	Definitions
$\mathcal{C}_i$	Client
id_i	Identity of client $\mathcal{C}_i$, where $id_i \in \mathrm{Sup}(\mathbb{T})$
pw_i	Password of client $\mathcal{C}_i$
h_ς	Secure and collision-free one-way chaotic hash function [47–52]
$\mathcal{U}_\mathcal{C}$	$\mathcal{C}_i$'s secret number
κ_1	$\mathcal{C}_i$'s chosen random number
$\mathcal{S}_j$	Trustworthy integrated EPR information system server
sk_i	$\mathcal{S}_j$'s secret key
α	$\mathcal{S}_j$'s secret number
β	Constant secret value of $\mathcal{S}_j$
κ_2	$\mathcal{S}_j$'s chosen random number
$\oplus$	Logical *XOR* operation
$\mathcal{U}\|\|\mathcal{V}$	u and v concatenation

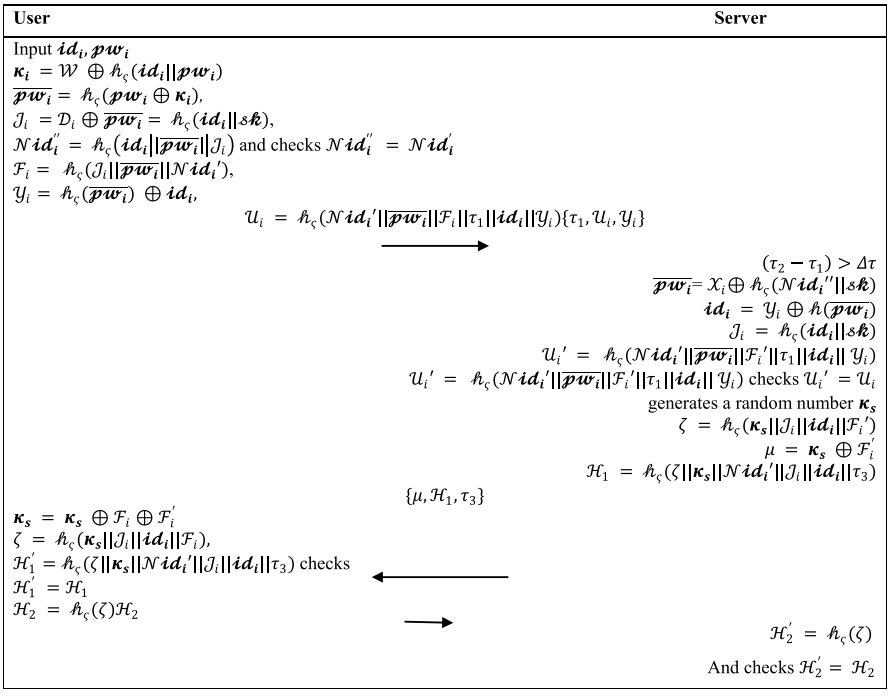

Fig. 2 Proposed scheme

4.1 Registration phase

Step 1: $\mathcal{C}_i$ chooses his identity, $id_i \in \text{Sup}(\mathbb{T})$, password pw_i, and random number κ_i, and computes $\overline{pw_i} = h_\varsigma(pw_i \oplus \kappa_i)$.$\mathcal{C}_i$, sends the registration request $\{id_i, \overline{pw_i}\}$ over a secure channel.

Step 2: Once the registration request is received, $\mathcal{S}_j$ checks the id_i's prescribed format and if id_i is invalid, registration request is aborted. Otherwise, $\mathcal{S}_j$ computes:

- $\mathcal{J}_i = h_\varsigma(sk||id_i)$,
- $\mathcal{D}_i = \mathcal{J}_i \oplus \overline{pw_i}$,
- $\mathcal{N}id'_i = h_\varsigma(id_i||\overline{pw_i}||\mathcal{J}_i)$,
- $\mathcal{X}_i = h_\varsigma(\mathcal{N}id'_i||sk) \oplus \overline{pw_i}$.

Finally, $\mathcal{S}_j$ stores $(\mathcal{D}_i, \mathcal{N}id'_i, h_\varsigma(.))$ on smart card and securely sends the smart card to $\mathcal{C}_i$. $\mathcal{S}_j$ stores $(\mathcal{N}id'_i, \mathcal{X}_i, bit)$ bit 0\1. Whenever $bit = 1$, which means the user is logged to the system, otherwise, $bit = 0$.

Step 3: On an arrival of smart card (SC), $\mathcal{W} = \kappa_i \oplus h_\varsigma(id_i||pw_i)$ is computed by the user and $\mathcal{W}$ is inserted on smart card. Lastly, $\{\mathcal{D}_i, \mathcal{N}id'_i, h_\varsigma(.), \mathcal{W}\}$ is preserved on smart card.

4.2 Login phase

If $\mathcal{C}_i$ wants to access EMR data from TMIS system then $\mathcal{C}_i$ need to logon by inserting smart card into the authenticating device, and need to supply id_i and pw_i. The following computation is performed by the smart card at the time of login into the server. Figure 1 shows the steps of login phase as well as authentication phase.

- $\kappa_i = \mathcal{W} \oplus h_\varsigma(id_i||pw_i)$,
- $\overline{pw_i} = h_\varsigma(pw_i \oplus \kappa_i)$,
- $\mathcal{J}_i = \mathcal{D}_i \oplus \overline{pw_i} = h_\varsigma(id_i||sk)$,
- $\mathcal{N}id''_i = h_\varsigma(id_i||\overline{pw_i}||\mathcal{J}_i)$.

The SC compares $\mathcal{N}id''_i$ and $\mathcal{N}id'_i$. If $\mathcal{N}id''_i = \mathcal{N}id'_i$ then inserted id_i, and pw_i are valid. Otherwise, session is terminated by SC. Therefore, computations performed by SC are

- $\mathcal{F}_i = h_\varsigma(\mathcal{J}_i||\overline{pw_i}||\mathcal{N}id'_i)$,
- $\mathcal{Y}_i = h_\varsigma(\overline{pw_i}) \oplus id_i$,
- $\mathcal{U}_i = h_\varsigma(\mathcal{N}id'_i||\overline{pw_i}||\mathcal{F}_i||\tau_1||id_i||\mathcal{Y}_i)$.

The SC determined the current timestamp τ_1 and $\mathcal{C}_i$ sends his/her login request $\{\tau_1, \mathcal{U}_i, \mathcal{Y}_i\}$ to $\mathcal{S}_j$ (medical server) via public channel.

4.3 Verification phase

If $\mathcal{C}_i$'s login request $\{\tau_1, \mathcal{U}_i, \mathcal{Y}_i\}$ is received by $\mathcal{S}_j$, following steps are performed by $\mathcal{C}_i$ and $\mathcal{S}_j$ confirms agreement for session-key and mutual authentication.

Step 1: At timestamp τ_2, $\mathcal{S}_j$ checks if $(\tau_2 - \tau_1) > \Delta\tau$, then login request is rejected by $\mathcal{S}_j$ otherwise it computes the following. Here, $\Delta\tau$ represents transmission delay maximum time.

- $\overline{pw_i} = \mathcal{X}_i \oplus h_\varsigma(\mathcal{N}id_i''||sk)$,
- $id_i = \mathcal{Y}_i \oplus h_\varsigma(\overline{pw_i})$,
- $\mathcal{J}_i = h_\varsigma(id_i||sk)$,
- $\mathcal{F}_i' = h_\varsigma(\mathcal{J}_i||\overline{pw_i}||\mathcal{N}id_i')$,
- $\mathcal{U}_i' = h_\varsigma(\mathcal{N}id_i'||\overline{pw_i}||\mathcal{F}_i'||\tau_1||id_i||\mathcal{Y}_i)$.

$\mathcal{S}$ compares $\mathcal{U}_i'$ and $\mathcal{U}_i$, if $\mathcal{U}_i' \neq \mathcal{U}_i$ then, session is terminated by $\mathcal{S}$; otherwise, $\mathcal{C}$ declare to be legitimate user.

Step 2: Random number κ_s is generated by $\mathcal{S}$ and perform the following computations.

- $\zeta = h_\varsigma(\kappa_s||\mathcal{J}_i||id_i||\mathcal{F}_i')$,
- $\mathcal{H}_1 = h_\varsigma(\zeta||\kappa_s||\mathcal{N}id_i'||\mathcal{J}_i||id_i||\tau_3)$,
- $\mu = \kappa_s \oplus \mathcal{F}_i'$.

Step 3: Response message $\{\mu, \mathcal{H}_1, \tau_3\}$ is sent to $\mathcal{C}_i$ by $\mathcal{S}$ via public channel.

Step 4: After receiving response message $\{\mu, \mathcal{H}_1, \tau_3\}$ from server $\mathcal{S}$, $\mathcal{C}_i$ computes.

- $\kappa_s = \kappa_s \oplus \mathcal{F}_i \oplus \mathcal{F}_i'$,
- $\zeta = h_\varsigma(\kappa_s||\mathcal{J}_i||id_i||\mathcal{F}_i)$,
- $\mathcal{H}_1' = h_\varsigma(\zeta||\kappa_s||\mathcal{N}id_i'||\mathcal{J}_i||id_i||\tau_3)$.

$\mathcal{C}_i$ compares $\mathcal{H}_1'$ and $\mathcal{H}_1$. If $\mathcal{H}_1' = \mathcal{H}_1$ then, authentication of $\mathcal{S}$ and ζ is performed; Otherwise, session is terminated. $\mathcal{C}_i$ computes, $\mathcal{H}_2 = h_\varsigma(\zeta)$ and $\mathcal{H}_2$ is sent to user.

Step 5: $\mathcal{S}$ computes $\mathcal{H}_2' = h_\varsigma(\zeta)$ and checks $\mathcal{H}_2' = \mathcal{H}_2$, If valid session key is hold by $\mathcal{S}$.

4.4 Password change phase

It is always a good practice that the client $\mathcal{C}_i$ should regularly change her/his password in order to improve protection. Assume that the client $\mathcal{C}_i$ wants to change her/his original password pw_i by a new changed password $pw_{i_{\text{new}}}$. To offer more security, password pw_i change is allowed to $\mathcal{C}_i$ and new password ($pw_{i_{\text{new}}}$) can be set. To do so, $\mathcal{C}_i$ inserts *SC* into an authenticating terminal, and then *SC* update password to $pw_{i_{\text{new}}}$ by performing following steps.

1. random number κ_i as $\kappa_i = \mathcal{W} \oplus \hbar_\varsigma(id_i||pw_i)$ is retrieved by SC and computes
   - $\overline{pw_i} = \hbar_\varsigma(pw_i \oplus \kappa_i)$,
   - $\mathcal{J}_i = \mathcal{D}_i \oplus \overline{pw_i} = \hbar_\varsigma(id_i||\jmath k)$,
   - $\mathcal{N}id_i'' = \hbar_\varsigma(id_i||\overline{pw_i}||\mathcal{J}_i)$

   SC checks for the equality of $\mathcal{N}id_i''$ and $\mathcal{N}id_i'$. If $\mathcal{N}id_i'' \neq \mathcal{N}id_i'$ then, no password update performed by SC. Otherwise, inserted id_i and pw_i are correct and hence new password is entered by $\mathcal{C}_i$ on asking SC.
2. $\mathcal{C}_i$ enters a new password $pw_{i_{\text{new}}}$. Later, SC computes
   - $\overline{pw}_{i_{\text{new}}} = \hbar_\varsigma(pw_{i_{\text{new}}} \oplus \kappa_i)$,
   - $\mathcal{N}id'_{i_{\text{new}}} = \hbar_\varsigma(id_i||\overline{pw}_{i_{\text{new}}})$,
   - $\mathcal{W}_{\text{new}} = \kappa_i \oplus \hbar_\varsigma(id_i||pw_{i_{\text{new}}})$,
   - $\mathcal{D}_{\text{new}} = \mathcal{D}_i \oplus \overline{pw}_{i_{\text{new}}} \oplus \overline{pw}_i$.

Finally, SC replaces $\mathcal{D}_{\text{new}}$, $\mathcal{W}_{\text{new}}$, and $\mathcal{N}id'_{i_{\text{new}}}$ instead of $\mathcal{D}_i, \mathcal{W}$, and $\mathcal{N}id_i'$, respectively. Here, random number κ_i can be changed by $\mathcal{C}_i$.

5 Security Analysis

This section is devoted to show the security proof of proposed scheme in RO model. Subsequently, the proof of correctness is also presented using BAN [55] logic for the same.

5.1 Formal security analysis

Here, RO model is utilized to propose the formal security analysis related to proposed scheme.

Definition 1 Secure and collision-resistant hash function based on chaotic maps [56].

It $Adv_{\mathcal{A}}^{CHASH}(t)$ denotes an adversary (attacker), then finding collision in chaotic hash function $\hbar_\varsigma(.)$ is an advantage to adversary $\mathcal{A}$ is as follows:

$$Adv_{\mathcal{A}}^{CHASH}(t) = \Pr\left[(\varkappa, \varkappa^*)\right] \Leftarrow \mathcal{A} : \varkappa \neq \varkappa^* and \hbar_\varsigma(\varkappa) = \hbar_\varsigma(\varkappa^*)],$$

Probability of occurrence of E is $Pr[E]$ in random space, and $(\varkappa, \varkappa^*) \Leftarrow A$ indicate that $(\varkappa, \varkappa^*)$ is chosen by $\mathcal{A}$ randomly. If $\varepsilon > 0$ then chaotic hash function resists the collision, we have $Adv_{\mathcal{A}}^{CHASH}(t) \leq \varepsilon$.

Following RO is chosen for formal security analysis of proposed scheme:

Reveal String $\varkappa$ is produced by the oracle unconditionally from the respective $\mathcal{Y} = \hbar_\varsigma(\varkappa)$ (chaotic hash value).

The formal security is offered by the Theorems 1 and 2, respectively, for proposed scheme which is protective against any adversary.

Theorem 1 *One-way chaotic hash function $\hbar_\varsigma(.)$ assumed to be an oracle, so proposed scheme is secure against the authenticate user's ($\mathcal{C}_i$) identity (id_i), server's ($\mathcal{S}_j$) private key ($\jmath\hbar$) and $\mathcal{C}_i$, $\mathcal{S}_j$ session key ζ.*

Proof We assume that $\mathcal{A}$ has the capability to extract id_i of $\mathcal{C}_i$ (legitimate user), $\jmath\hbar$ (private key) of $\mathcal{S}_j$ (server), and ζ (session key) between $\mathcal{C}_i$ and $\mathcal{S}_j$. The $\mathcal{A}$ utilizes Reveal oracle to execute $\text{EXP1}_{\text{SAKTMIS}}^{CHASH}$ (experimental algorithm) for proposed key agreement authentication based on biometric in multi-server environment, i.e., SAKTMIS, which is presented in Algorithm 1.

Success probability, $Succ1_{\text{SAKTMIS}}^{CHASH} = [\Pr[\text{EXP1}_{\text{SAKTMIS}}^{CHASH} = 1] - 1]$ is described for $\text{EXP1}_{\text{SAKTMIS}}^{CHASH}$. Then the advantage becomes $Adv_{\text{SAKTMIS}}^{CHASH}(t_1, q_{\mathcal{R}}) = max_A\{Succ1_{\text{SAKTMIS}}^{CHASH}\}$, Advantage function using t (execution time) and $q_{\mathcal{R}}$ (No. of RO reveal queries) is maximized on $\mathcal{A}$. If $Adv_{\text{SAKTMIS}}^{CHASH}(t_1, q_{\mathcal{R}}) < \varepsilon$, for smaller $\varepsilon > 0$ then we declare proposed scheme is protective to $\mathcal{A}$ while trying to extract id_i, $\jmath\hbar$ and ζ.

Experiment on Algorithm 1 If $\mathcal{A}$ is capable to invert $\hbar_\varsigma(.)$ (hash function), then $\mathcal{A}$ wins the game by having id_i, $\jmath\hbar$ and ζ. However, it is hard to invert as per Definition 1, moreover, to invert $\hbar_\varsigma(.)$ the problem is computationally not feasible. Since $Adv_A^{CHASH}(t) \le \varepsilon$, for smaller $\varepsilon > 0$, we have $Adv_A^{CHASH}(t_1, q_{\mathcal{R}}) \le \varepsilon$, which is does not depend on the earlier. Therefore, proposed scheme is fully protective against $\mathcal{A}$ while extracting id_i, $\jmath\hbar$ and ζ.

Algorithm 1. $\text{EXP1}_{\text{SAKTMIS}}^{CHASH}$

1: Message of login request is eavesdropped $\{\tau_1, \mathcal{U}_i, \mathcal{Y}_i\}$ at the time of login phase, here $\mathcal{U}_i = \hbar_\varsigma(\mathcal{N}id_i' || \overline{pw_i} || \mathcal{F}_i || \tau_1 || id_i || \mathcal{Y}_i)$, $\mathcal{Y}_i = \hbar_\varsigma(\overline{pw_i}) \oplus id_i$, $\overline{pw_i} = \hbar_\varsigma(pw_i \oplus \kappa_i)$, $\mathcal{F}_i = \hbar_\varsigma(\mathcal{J}_i || \overline{pw_i} || \mathcal{N}id_i')$, $\mathcal{N}id_i'' = \hbar_\varsigma(id_i || \overline{pw_i} || \mathcal{J}_i)$,
2. Reveal oracle is called on input $\mathcal{U}_i$ to extract $id_i, \mathcal{F}_i \mathcal{Y}_i, \overline{pw_i}, \mathcal{N}id_i, \tau_1$ as $(\mathcal{N}id_i' || \overline{pw_i}' || \mathcal{F}_i' || \tau_1' || id_i' || \mathcal{Y}_i') \leftarrow reveal(\mathcal{U}_i)$
3. computes $\mathcal{Y}_i' = id_i' \oplus \hbar_\varsigma(\overline{pw_i}')$
4. If $(\mathcal{Y}_i' = \mathcal{Y}_i)$ then
5. Accepted, id_i' is the correct id_i of user
6. Authentication message is eavesdropped $(\mu, \mathcal{H}_1, \tau_3)$ during the authentication phase, where $\mathcal{H}_1 = \hbar_\varsigma(\zeta || \kappa_s || \mathcal{N}id_i' || \mathcal{J}_i || id_i || \tau_3)$, $\mu = \kappa_s \oplus \mathcal{F}_i'$, $\mathcal{J}_i = \hbar_\varsigma(id_i || \jmath\hbar)$
7. Reveal oracle is called on input $\mathcal{H}_2$ to extract $\zeta, \kappa_s, \mathcal{N}id_i, id_i, \mathcal{J}_i, \tau_3$ as $(\zeta' || \kappa_s' || \mathcal{N}id_i' || \mathcal{J}_i' || id_i' || \tau_3') \leftarrow reveal(\mathcal{H}_1)$
8. Reveal oracle is called on input $\lfloor$ to extract $\jmath\hbar$(private key) of $\mathcal{S}$ (server) as $(id_i | \jmath\hbar) \leftarrow$ **reveal**$(\mathcal{J}_i)$
9. Calculates $\zeta'' = \hbar_\varsigma(\kappa_s' || \mathcal{J}_i' || id_i' || \mathcal{F}_i')$, $\mathcal{H}_1'' = \hbar_\varsigma(\zeta' || \kappa_s' || \mathcal{N}id_i' | \mathcal{J}_i' || id_i' || \tau_3')$
10. If $(\mathcal{H}_1' = \mathcal{H}_1'')$ than
11. Correct identity id_i (user) is accepted as id_i, $\varkappa$, and ζ, $\jmath\hbar$ (private key) of $\mathcal{S}$ (server), and ζ (session key) among $\mathcal{C}_i$ and $\mathcal{S}_|$, respectively.
return 1 (i.e., Success)
12: else
13: return 0 (i.e., Failure)
14: end if
15: else
16: return 0 (i.e., Failure)

Theorem 2 *One-way chaotic hash function $\hbar_{\varsigma}(.)$ assumed to be an oracle, the proposed scheme stands protective against $\mathcal{A}$ for extracting pw_i (password) of $\mathcal{C}_i$ (user), in the situation of smart card ($\mathcal{C}_i's$) lost or stolen by $\mathcal{A}$.*

Proof We assume that $\mathcal{A}$ has the capability to extract pw_i of $\mathcal{C}_i$ (user), the extracted information is stored on smart card of $\mathcal{C}_i$. So, experiment $\text{EXP2}^{CHASH}_{\text{SAKTMIS}}$ is executed by $\mathcal{A}$ presented in Algorithm 2.

The $Succ2^{CHASH}_{\text{SAKTMIS}} = [\Pr[\text{EXP2}^{CHASH}_{\text{SAKTMIS}} = 1] - 1]$ is the success probability to execute $\text{EXP2}^{CHASH}_{\text{SAKTMIS}}$ and $Adv2^{CHASH}_{\text{SAKTMIS}}(t_2, q_{\mathcal{R}}) = max_A\{Succ2^{CHASH}_{\text{SAKTMIS}}\}$, advantage of $\text{EXP2}^{CHASH}_{\text{SAKTMIS}}$, where advantage function using t (execution time) and $q_{\mathcal{R}}$ (No. of RO reveal queries) is maximized on $\mathcal{A}$. If $Adv2^{CHASH}_{\text{SAKTMIS}}(t_2, q_{\mathcal{R}}) < \varepsilon$, and $\varepsilon > 0$ is sufficiently smaller than our scheme offers security against $\mathcal{A}$ for extracting pw_i of $\mathcal{C}_i$.

Assuming, all secrets $\{\mathcal{D}_i, \mathcal{N}id_i', \hbar_{\varsigma}(.), \mathcal{W}\}$ retrieved by $\mathcal{A}$ from $\mathcal{C}_i$'s smart card.

Experiment on Algorithm 2 If $\mathcal{A}$ is capable to invert $\hbar_{\varsigma}(.)$ (hash function), by deriving pw_i of $\mathcal{C}_i$, $\mathcal{A}$ wins the game. By the definition of chaotic hash function, $Adv^{CHASH}_{\mathcal{A}}(t) \leq \varepsilon$, with smaller $\varepsilon > 0$. We have $Adv^{CHASH}_{\mathcal{A}}(t_2, q_{\mathcal{R}}) \leq \varepsilon$, as it is dependent on $Adv^{CHASH}_{\mathcal{A}}(t)$. So, computationally it's impractical to invert $\hbar_{\varsigma}(.)$. Hence, our scheme is protective against $\mathcal{A}$ for extracting pw_i of $\mathcal{C}_i$ from smart card under lost or stolen scenario.

Algorithm 2. $\text{EXP2}^{HASH}_{BAKATN}$

1. Secret information is extracted $\{\mathcal{D}_i, \mathcal{N}id_i', \hbar_{\varsigma}(.), \mathcal{W}\}$ from smart card SC_i of $\mathcal{C}_i$ when lost or stolen based on attacks described in [47, 48]. Where $\mathcal{D}_i = \mathcal{J}_i \oplus \overline{pw_i}, \mathcal{N}id_i' = \hbar_{\varsigma}(id_i||\overline{pw_i}||\mathcal{J}_i), \mathcal{W} = \kappa_i \oplus \hbar_{\varsigma}(id_i||pw_i)$.
2. Reveal oracle is called on input $\mathcal{N}id_i'$, to extract $\overline{pw_i}$, $\mathcal{J}_i$ and id_i as $(id_i||\overline{pw_i}||\mathcal{J}_i) \leftarrow$ **reveal**(M_i),
3. Reveal oracle is called on input $\overline{pw_i}$ to extract pw_i, κ_i and id_i as $(pw_i, \kappa_i) \leftarrow$ **reveal**$(\overline{pw_i})$,
4. Computes $\mathcal{W}^* = \kappa_i \oplus \hbar_{\varsigma}(id_i||pw_i)$
5. if $(\mathcal{W}^* = \mathcal{W})$ then
6. pw_i is correct password of $\mathcal{C}_i$.
7: return 1 (i.e., Success)
8: else
9: return 0 (i.e., Failure)
10: end if

5.2 BAN logic for authentication proof

The authentication scheme or protocol can be analyzed using the BAN [55] logic. Generally, BAN logic is adapted to validate the authentication protocols as well as protocols for key establishment. Table 2 shows the various notations used and logical rules applied in BAN logic.

Idealized form of protocol messages is as follows:

Table 2 Various notations and BAN logic rules

$\mathcal{Q} \mid\equiv$: The principal $\mathcal{Q}$ believes a statement $\mathcal{U}$, or $\mathcal{Q}$ is entitled to believe $\mathcal{U}$
$\#(\mathcal{U})$: The formula $\mathcal{U}$ is fresh
$\mathcal{Q} \Rightarrow$: The principal $\mathcal{Q}$ has competence over the statement $\mathcal{U}$
$\mathcal{Q} \mid\sim$: The principal $\mathcal{Q}$ once said the statement $\mathcal{U}$
$<\mathcal{U}>$: The formula $\mathcal{U}$ combined with the formula $\mathcal{V}$
$\{\mathcal{U}\}_{\mathcal{V}}$: The formula is encrypted with the key $\boldsymbol{\kappa}$
$(\mathcal{U})_{\mathcal{V}}$: The formula is hash with the key $\boldsymbol{\kappa}$
$\mathcal{Q} \leftarrow \boldsymbol{\kappa} \rightarrow$: The principal's and use the shared key $\boldsymbol{\kappa}$ to encrypt data. The key $\boldsymbol{\kappa}$ will never be disclosed by any principal except $\mathcal{Q}$ and $\mathcal{P}$
The message-meaning rule: $\frac{\mathcal{Q} \mid\equiv q \overset{\kappa}{\longleftrightarrow} \mathcal{P}, q \textbf{sees} \{\mathcal{U}\}_{\boldsymbol{\kappa}}}{\mathcal{Q} \mid\equiv \mathcal{P} \mid\sim \mathcal{U}}$
The freshness-conjuncatenation rule: $\frac{\mathcal{Q} \mid\equiv \#(\mathcal{U})}{\mathcal{Q} \mid\equiv \#(\mathcal{U}, \mathcal{V})}$
The nonce-verification rule: $\frac{\mathcal{Q} \mid\equiv \#(\mathcal{U}), q \mid\equiv \mathcal{P} \mid\sim \mathcal{U}}{\mathcal{Q} \mid\equiv \boldsymbol{Q} \mid\equiv \mathcal{U}}$
The jurisdiction rule: $\frac{\mathcal{Q} \mid\equiv \mathcal{P} \Rightarrow \equiv \mathcal{U}, \mathcal{Q} \mid\equiv \mathcal{P} \mid\equiv \mathcal{U}}{\mathcal{Q} \mid\equiv \mathcal{U}}$

Message 1. $\mathcal{C}_i \rightarrow \mathcal{S}$: $\left(\left(id_i\right)_{\hbar_\varsigma(pw_i \oplus \kappa_i)}, (id_i || \mathcal{Y}_i || \mathcal{N}id_i' || \tau_1)_{\hbar_\varsigma(\hbar_\varsigma(id_i || \jmath k) || \hbar_\varsigma(pw_i \oplus \kappa_i)}, \tau_1\right)$

Message 2. $\mathcal{S} \rightarrow \mathcal{C}_i$: $\left(\mathcal{S} \overset{\kappa_s}{\longleftrightarrow} \mathcal{C}_i\right)_{\hbar_\varsigma(\hbar_\varsigma(id_i || \jmath k) || \hbar_\varsigma(pw_i \oplus \kappa_i))}, (\mathcal{C}_i \overset{\zeta}{\longleftrightarrow} \mathcal{S} || \mathcal{S} \overset{\kappa_s}{\longleftrightarrow} \mathcal{C}_i || \mathcal{N}id_i' || id_i || \tau_3)_\zeta$

Message 3. $\mathcal{S} \rightarrow \mathcal{C}_i$: $(\kappa_s || \mathcal{J}_i || id_i || \mathcal{F}_i')_\zeta$

5.2.1 Assumption

Following assumption are adapted in BAN logic to perform formal analysis:

$A_1)$ $\mathcal{C}_i \mid\equiv \#(\tau_1)$.

$A_2)$ $\mathcal{C}_i \mid\equiv (\mathcal{C}_i \overset{\hbar_\varsigma(\hbar_\varsigma(id_i || \jmath k) || \hbar_\varsigma(pw_i \oplus \kappa_i))}{\longleftrightarrow} \mathcal{S})$.

$A_3)$ $\mathcal{S} \mid\equiv (\mathcal{C}_i \overset{\hbar_\varsigma(\hbar_\varsigma(id_i || \jmath k) || \hbar_\varsigma(pw_i \oplus \kappa_i))}{\longleftrightarrow} \mathcal{S})$.

$A_4)$ $\mathcal{C}_i \mid\equiv (\mathcal{C}_i \overset{\hbar_\varsigma(pw_i \oplus \kappa_i)}{\longleftrightarrow} \mathcal{S})$.

$A_5)$ $\mathcal{S} \mid\equiv (\mathcal{C}_i \overset{\hbar_\varsigma(pw_i \oplus \kappa_i))}{\longleftrightarrow} \mathcal{S})$.

$A_6)$ $\mathcal{S}_{\mathcal{J}} \mid\equiv \#(\tau_3)$.

$A_7)$ $\mathcal{S}_{\mathcal{J}} \mid\equiv \mathcal{C}_i \mid \equiv \mathcal{C}_i \overset{\hbar_\varsigma(\hbar_\varsigma(id_i || \jmath k) || \hbar_\varsigma(pw_i \oplus \kappa_i))}{\longleftrightarrow} \mathcal{S}$

$A_8)$ $\mathcal{C}_i \mid \equiv \mathcal{S}_{\mathcal{J}} \mid \equiv \mathcal{C}_i \overset{\hbar_\varsigma(\hbar_\varsigma(id_i || \jmath k) || \hbar_\varsigma(pw_i \oplus \kappa_i))}{\longleftrightarrow} \mathcal{S}$

5.2.2 Analysis

Proposed scheme's verification can be performed based on above assumptions and rules given in Table 3 related to BAN logic.

Lemma 1 *The authenticity of login message of $\mathcal{C}_i$ could be correctly verified by $\mathcal{S}$ (server).*

Table 3 Comparison based on security features/attacks

S. no	Security attack\scheme	Chiou et al. [60]	Ravanbakhsh and Nazari [61]	Ostad et al. [62]	Proposed scheme
1	Stolen smart card attack	Yes	No	No	Yes
2	Offline password guessing attack	Yes	Yes	Yes	Yes
3	User's stolen/lost smart card attack	No	Yes	Yes	Yes
4	Denial-of-service attack	No	Yes	Yes	Yes
5	Replaying attack	Yes	Yes	Yes	Yes
6	Stolen verifier attack	No	–	–	Yes
7	Impersonation attack	No	Yes	Yes	Yes
8	Privileged insider attack	No	Yes	Yes	Yes
9	Forward secrecy	Yes	Yes	Yes	Yes
10	Many logged-in users' attacks	Yes	No	No	Yes

Proof Login message send by $\mathcal{C}_i$ to $\mathcal{S}$. Then, timestamp and other values are received by $\mathcal{S}$ and message source's correctness can be proved as follows:

Message 1. $\mathcal{C}_i \rightarrow \mathcal{S}$: $\left(\left(id_i\right)_{\hbar_\varsigma(pw_i \oplus \kappa_i)}, (id_i||\mathcal{Y}_i||\mathcal{N}id_i'||\tau_1)_{\hbar_\varsigma(\hbar_\varsigma(id_i||\jmath\hbar)||\hbar(pw_i \oplus \kappa_i)}, \tau_1\right)$

S_1) $\mathcal{S} \lhd$: $\left(id_i\right), (id_i||\mathcal{Y}_i||\mathcal{N}id_i'||\tau_1), \tau_1$// According to seeing rule.

S_2) $\mathcal{S} \models \mathcal{C}_i| \sim \left(id_i\right), (id_i||\mathcal{Y}_i||\mathcal{N}id_i'||\tau_1), \tau_1$// According to A_3, A_5, S_1, message-meaning rule.

S_3) $\mathcal{S} \models \mathcal{C}_i \models \left(id_i\right), (id_i||\mathcal{Y}_i||\mathcal{N}id_i'||\tau_1), \tau_1$// According to A_1, the freshness-conjuncatenation rule to S_2.

S_4) $\mathcal{S} \models \tau_1$// According to A_1, S_3.

The fresh timestamp corresponding to the message is considered by $\mathcal{S}$ (server). Hence, message source is correct is proved.

Lemma 2 *The correctness of message responded by $\mathcal{S}$ (server) can be verified by $\mathcal{C}_i$ (user).*

Proof Once the correctness of authenticate $\mathcal{C}_i$'s (user's) login message is confirmed, which consist of $\mathcal{S}$'s timestamp. Then, authenticity of $\mathcal{S}$'s message can be proved by $\mathcal{C}_i$ is shown as follows:

Message 2: $\mathcal{S} \rightarrow \mathcal{C}_i$: $\left(\mathcal{S} \overset{\kappa_s}{\longleftrightarrow} \mathcal{C}_i\right)_{\hbar_\varsigma(\hbar_\varsigma(id_i||\jmath\hbar)||\hbar_\varsigma(pw_i \oplus \kappa_i))}$, $(\mathcal{C}_i \overset{\zeta}{\longleftrightarrow} \mathcal{S}||\mathcal{S} \overset{\kappa_s}{\longleftrightarrow} \mathcal{C}_i||\mathcal{N}id_i'||id_i||\tau_3)_\zeta$

S_5) $\mathcal{C}_i \lhd \left(\mathcal{S} \overset{\kappa_s}{\longleftrightarrow} \mathcal{C}_i\right)_{\hbar_\varsigma(\hbar_\varsigma(id_i||\jmath\hbar)||\hbar_\varsigma(pw_i \oplus \kappa_i))}, (\mathcal{C}_i \overset{\zeta}{\longleftrightarrow} \mathcal{S}||\mathcal{S} \overset{\kappa_s}{\longleftrightarrow} \mathcal{C}_i||\mathcal{N}id_i'||id_i||\tau_3)_\zeta$

S_6) Based on assumption $A3$, S_5 message meaning rule is applied hence we get.

$\mathcal{C}_i \models \mathcal{S}| \sim \left(\mathcal{S} \overset{\kappa_s}{\longleftrightarrow} \mathcal{C}_i\right), (\mathcal{C}_i \overset{\zeta}{\longleftrightarrow} \mathcal{S}||\mathcal{S} \overset{\kappa_s}{\longleftrightarrow} \mathcal{C}_i||\mathcal{N}id_i'||id_i||\tau_3)_\zeta$

S_7) Based on assumption $A2$, freshness rule is applied hence we get.
$\mathcal{C}_i \mid\equiv \mathcal{S}\mid \equiv \left(\mathcal{S} \overset{\kappa_s}{\longleftrightarrow} \mathcal{C}_i\right), (\mathcal{C}_i \overset{\zeta}{\longleftrightarrow} \mathcal{S}||\mathcal{S} \overset{\kappa_s}{\longleftrightarrow} \mathcal{C}_i||\mathcal{N}id_i'||id_i||\tau_3)_\zeta$.
S_8) By using $A3$, $A6$ and S_7, jurisdiction rule is applied hence we get $\mathcal{S}\mid \equiv \mathcal{S} \overset{\kappa_s}{\longleftrightarrow} \mathcal{C}_i, \tau_3$.
This shows that correct verification of message source as well as its freshness could be done by $\mathcal{C}_i$.

Lemma 3 *If authentication for message holds then common session key is computed by $\mathcal{C}_i$ and $\mathcal{S}$.*

Proof As per proposed scheme, after verifying timestamps and freshness of random number, $\mathcal{C}_i$ and $\mathcal{S}$ can compute $\zeta = \hbar_\varsigma(\kappa_s||\mathcal{J}_i||id_i||\mathcal{F}_i')$ (session key). By utilizing Lemmas 1 and 2, authenticity of $\mathcal{C}_i$ and $\mathcal{S}$ among them is correctly verified. So, the unique session key generated using random number or fresh timestamps ensures the utilization of fresh session key for new session. The correct computation of negotiated session key is generated is believed by $\mathcal{C}_i$ and $\mathcal{S}$ shown as follows:

S_9) By using $\zeta = \hbar_\varsigma(\kappa_s||\mathcal{J}_i||id_i||\mathcal{F}_i')$ we could get $\mathcal{C}_i \mid\equiv \mathcal{C}_i \overset{\zeta}{\longleftrightarrow} \mathcal{S}_j$.
S_{10}) As per message 3 we get $\mathcal{S} \lhd (\mathcal{S} \overset{\kappa_s}{\longleftrightarrow} \mathcal{C}_i||\mathcal{J}_i||id_i||\mathcal{F}_i')_\zeta$.
S_{11}) $\mathcal{S} \mid\equiv \mathcal{C}_i\mid \sim (\mathcal{S} \overset{\kappa_s}{\longleftrightarrow} \mathcal{C}_i||\mathcal{J}_i||id_i||\mathcal{F}_i')_\zeta$// According to S_{10}, A_3.
S_{12}) $\mathcal{S} \mid\equiv \mathcal{C}_i \mid\equiv (\mathcal{S} \overset{\kappa_s}{\longleftrightarrow} \mathcal{C}_i||\mathcal{J}_i||id_i||\mathcal{F}_i')$.
S_{13}) According to the $\zeta = \hbar_\varsigma(\kappa_s||\mathcal{J}_i||id_i||\mathcal{F}_i')$ we could get $\mathcal{C}_i \mid\equiv \mathcal{C}_i \overset{\zeta}{\longleftrightarrow} \mathcal{S}_j$.

5.3 Discussions on attacks

5.3.1 Stolen smart card attack

Assume that the client $\mathcal{C}_i$'s smart card is lost or stolen. As described in threat model [53]. Here, by using attacks described in [17, 53, 54], however, if the attacker uses the found smart card in order to login to the server $\mathcal{S}_j$, the attacker has to obtain/guess the correct password pw_i of the client $\mathcal{C}_i$. Attacker extract stored information on the smart card $\{\mathcal{D}_i, \mathcal{N}id_i', \hbar_\varsigma(.), \mathcal{W}\}$, once he/she find or stolen the smart card. Attacker deduce correct pw_i of $\mathcal{C}_i$ to login to $\mathcal{S}_j$. However, we prove that valid pw_i and id_i is cannot be computed by attacker. As a result, the attacker is unable to obtain the correct password of the client $\mathcal{C}_i$ and hence, our presented authentication protocol protects stolen smart card attacks.

5.3.1.1 Offline password guessing attack In offline mode, to find user's password, attacker must have random number κ_i, id_i and secret key d. The user's pw_i can be used only inside $\mathcal{Y}_i = \hbar_\varsigma(\overline{pw_i}) \oplus id_i$ and $\mathcal{U}_i = \hbar_\varsigma(\mathcal{N}id_i'||\overline{pw_i}||\mathcal{F}_i||\tau_1||id_i||\mathcal{Y}_i)$. We observe that the guessing of correct password by an adversary need to find correct values id_i and pw_i simultaneously but finding correct id_i with exact ℓ_1 bits length and pw_i with exact ℓ_2 characters length concurrently is the probability is $2^{-\ell_1-6\ell_2}$. So, with probability $2^{-\ell_1-6\ell_2}$, the guessing is negligible and also finding in polyno-

mial time [57] is not possible. Hence, we conclude the proposed scheme is protective for offline password guessing attack.

5.3.1.2 User's stolen/lost smart card is untraceable While login and authentication phase, messages are transmitted such as $\{\tau_1, \mathcal{U}_i, \mathcal{Y}_i\}$, $\{\mu, \mathcal{H}_1, \tau_3\}$ and $\{\mathcal{H}_2\}$, and can be intercepted by adversary and $\{\mathcal{D}_i, \mathcal{N}id_i', \hbar_\varsigma(.), \mathcal{W}\}$ can be extracted from *SC*. The user's identity can be found inside $\mathcal{Y}_i = \hbar_\varsigma(\overline{pw_i}) \oplus id_i$. Moreover, without id_i and pw_i, it is not possible for attacker to obtain user's identity correctly. Thus, it is impossible to do in polynomial time [57]. Eventually, holder's plaintext identity is not stored in *SC*. So, holder's tracing based on smart card is not allowed by the proposed scheme.

5.3.2 Denial-of-service attack

When $\mathcal{C}_i$ inserts his identity id_i and password pw_i, the login message is not computed instantly by *SC* in proposed scheme. The correctness of id_i and pw_i which is inserted is firstly checked. *SC* retrieves the random number $\kappa_i = \mathcal{W} \oplus \hbar_\varsigma(id_i || pw_i)$ and computes $\overline{pw_i} = \hbar_\varsigma(pw_i \oplus \kappa_i) \mathcal{N}id_i'' = \hbar_\varsigma(id_i || \overline{pw_i} || \mathcal{J}_i)$ and compares $\mathcal{N}id_i''$ with $\mathcal{N}id_i'$ which is stored on *SC*. The password is correct, if $\mathcal{N}id_i'' = \mathcal{N}id_i'$. Otherwise, incorrect password is identified and session is epilogue by *SC*. So, by using wrong password, the legitimate user is also not able to activate his/her *SC*. This works as a prevention mechanism for user not to insert false identifiers by mistake. Now, healthcare services can be accessed by the user without facing any problem of denial-of-service. Therefore, denial-of-service attack is easily handled by proposed scheme.

5.3.3 Replaying attack

The protection against replaying attack by the adversary is tackle by using timestamps, when login message is replays to $\mathcal{S}$. Invalid timestamp τ_i (resp. τ_S) is detected by $\mathcal{S}$ (resp. $\mathcal{C}_i$) when an adversary replays ℓ_1 (resp. ℓ_1').

5.3.4 Stolen verifier attack

The cipher-text $(\mathcal{N}id_i', \mathcal{X}_i,$ bit) with $\mathcal{X}_i = \hbar_\varsigma(\mathcal{N}id_i' || \mathcal{SK}) \oplus \overline{pw_i}$ and $\mathcal{N}id_i' = \hbar_\varsigma(id_i || \overline{pw_i} || \mathcal{J}_i)$ is stored by the server on its database. Secret key $\mathcal{SK}$ and $\overline{pw_i}$ is only known to $\mathcal{S}_j$; hence, storing the values into the database is the sole responsibility of $\mathcal{S}_j$. Thus, stolen verifier attack in not vulnerable to proposed scheme.

5.3.5 Impersonation attack

The $\mathcal{S}_j$ or $\mathcal{C}_i$ are impersonated by the attacker under impersonate attack. To do so, the valid login request $\{\tau_1, \mathcal{U}_i, \mathcal{Y}_i\}$ is forges by an adversary, where $\mathcal{U}_i = \hbar_\varsigma(\mathcal{N}id_i' || \overline{pw_i} || \mathcal{F}_i || \tau_1 || id_i || \mathcal{Y}_i)$ and $\mathcal{Y}_i = \hbar_\varsigma(\overline{pw_i}) \oplus id_i$. However, without the values of id and pw, $\mathcal{U}_i$ is not able to computed by an adversary, similar to

Sect. 3.3.1.1, user's correct password guess is fails here by the adversary. So, login request says to be correct cannot be generated by an adversary in the scenario when $\mathcal{C}_i$'s smart card secret information $\{\mathcal{D}_i, \mathcal{N}id'_i, \hbar_\varsigma(.), \mathcal{W}\}$ is extracted by an adversary. Hence, proposed scheme smartly prevents from impersonation attack.

If $\mathcal{S}_j$ (server) is impersonated by the attacker. To do so, correct response message $\{\mu, \mathcal{H}_1, \tau_3\}$ where $\mathcal{H}_1 = \hbar_\varsigma(\zeta||\kappa_s||\mathcal{N}id'_i||\mathcal{J}_i||id_i||\tau_3)$ and $\mu = \kappa_s \oplus \mathcal{F}'_i$ is forged by the attacker. Here, attacker must have the secret key $\varkappa$ belongs to $\mathcal{S}$. So, generation of valid response message by the attacker is not possible. Therefore, impersonation attack is prevented by proposed scheme.

5.3.6 Privileged insider attack

There is no provision of sending password in the form of plaintext by $\mathcal{C}_i$ in proposed scheme. Random number κ_i is utilized to send $\overline{pw_i} = \hbar_\varsigma(pw_i \oplus \kappa_i)$ by $\mathcal{C}_i$. Hence, no insider at $\mathcal{S}$ side obtains pw_i at the time of registration phase. Moreover, pw_i from $\overline{pw_i}$ cannot be retrieved; therefore, privileged insider attack is resisted by proposed scheme.

5.3.7 Forward secrecy

On leakage of $\varkappa$ (secret key) of server. Still, the session key (ζ) cannot be computed by an adversary, because user's identity is not known to the adversary to obtain $\zeta = \hbar_\varsigma(\kappa_s||\mathcal{J}_i||id_i||\mathcal{F}'_i)$. Hence, due to the lack of session key, proposed scheme maintain forward secrecy.

5.3.8 Many logged-in users' attacks

The attack under title signifies that other user knows the id_i (identity) and pw_i (password) in the scenario when user's *SC* is lost or stolen. Then, everyone having *SC* and pw_i (password for same *SC*) can simultaneously logged to $\mathcal{S}$ [58, 59]. However, $\mathcal{S}$ will not allow more users to access account of a legal user simultaneously. Here, under the assumption that non-registered users know the $\mathcal{C}_i$'s identity id_i, password pw_i and parameters $\{\mathcal{D}_i, \mathcal{N}id'_i, \hbar_\varsigma(.), \mathcal{W}\}$. However, $\mathcal{S}$ is maintaining field called "*status-bit*" in identity table, which restrict the simultaneously login on $\mathcal{S}$. For example, when first user login into $\mathcal{S}$. Then, status-bit is set to 1 by $\mathcal{S}$. Now, the request of login by second user on $\mathcal{S}$ is rejected, because the status-bit is already set to 1, indicates that someone is already login on the server. Thus, our scheme is also secured when many logged-in users attacks are performed on the system.

6 Performance comparison

The performance analysis and comparative study related to the security and functionality features supported by the proposed scheme presented in this section. In addition, proposed signature scheme's efficiency is compared to the current schemes described in Chiou et al. [60], Ravanbakhsh and Nazari [63], and Ostad et al. [65].

Table 4 Notations used for computational cost

Notation used	Meaning (Execution time)
T_{me}	One modular exponentiation operation
T_h	One-way hash function
T_s	Symmetric key encryption–decryption operation
T_m	One elliptic curve point multiplication
T_{chao}	Chebyshev chaotic map
T_p	One bilinear pairing operation
T_{ex}	Modular exponentiation in group

Table 5 Execution time for each operation

S. no	Notation used	Execution time (ms)
1	T_{me}	19.2
2	T_h	0.32
3	T_s	5.6
4	T_m	17.1
5	T_{chao}	0.32
6	T_p	496
7	T_{ex}	192

The proposed scheme has capability to address the problem of stolen smart card attack and offline password guessing attack, etc. Table 3 shows the comparison based on various security features supported by the proposed scheme. Table 3 also demonstrates that the proposed scheme is effective in handling various attacks discussed in Sect. 5. The comparison has been made based on computational time. The comparative analysis used the notations mentioned in Table 4. The study uses the computational cost given in He et al. [63], and moreover the time required by each operation is presented in Table 4. The computational cost for modular exponentiation operation and one bilinear pairing operation is taken as 192 ms, and 496 ms, respectively. The computational cost for chaotic hash function is taken as equal to general hash function. The signing stage and the verification stage are influencing the overall performance of the scheme. Therefore, in this study, we compared the computational cost for signing stage and the verification stage, because it is the most dominating factor. Table 5 presents an overview execution time for each operation of our scheme in this research work over the state-of-the-art schemes mentioned in the literature.

Table 6 demonstrates that our scheme is more efficient than Chiou et al. [60], Ravanbakhsh and Nazari [61], and Ostad et al. [62] based on the time required for the various phases. It is seen from Table 6 that the proposed scheme requires only 52.58 ms for the registration stage, 70.64 ms for the login stage, 70.64 ms for the verification stage, and 104.52 ms for the password change stage. The total computational cost for the proposed scheme is 298.38 ms which is very less as compared to the counterparts. In addition, Fig. 3 shows the pictorial representation of

Table 6 Comparison based on computational cost

S. no.	Scheme/phases	Registration phase	Login phase	Verification phase	Password change phase	Total cost (ms)
1	Chiou et al. [60]	$3T_p + 4T_s + 7T_h =$ 1512.64 ms	$4T_p + 4T_s + 12T_h =$ 2010.24 ms	$4T_m + 4T_p + 4T_s + 6T_h =$ 2076.72 ms	$2T_p + 2T_s + 8T_h =$ 1005.76 ms	6605.36
2	Ravanbakhsh and Nazari [61]	$5T_h + 5T_m + 2T_{ex} =$ 471.1 ms	$6T_h + 10T_m = 172.92$ ms	$5T_h + 6T_m = 188.1$ ms	$6T_h + 11T_m = 190.02$ ms	1022.14
3	Ostad et al. [62]	$7T_h + 2T_m + 3T_{ex} =$ 612.44 ms	$6T_h + 1T_m + 4T_{ex} =$ 787.02 ms	$6T_h + 4T_m + 10T_{ex} =$ 1990.32 ms	$3T_h + 4T_m + 12T_{ex} =$ 2373.36 ms	5763.14
4	Proposed scheme	$4T_{chao} + 3T_m = 52.58$	$7T_{chao} + 4T_m = 70.64$ ms	$7T_{chao} + 4T_m = 70.64$ ms	$6T_{chao} + 6T_m = 104.52$ ms	298.38

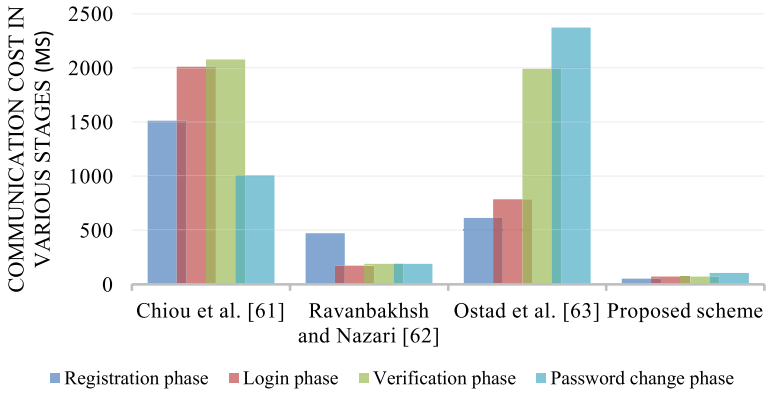

Fig. 3 Comparative analysis based on computational cost for various stages

comparative analysis and highlights the better performance of proposed scheme in comparison to current schemes.

7 Conclusions

In this article, we proposed an efficient lightweight and provably secure authentication scheme for client with anonymity for TMIS using chaotic hash function. We also, showed that the presented scheme is secure against very potential attacks such as stolen smart card attack, denial-of-service attack, replaying attack, stolen verifier attack, impersonation attack, privileged insider attack, forward secrecy, and many logged-in users' attacks. Moreover, this new system is secure via structured security verification. The formal and informal security analysis is performed on the proposed scheme to ensure no security breaches. In addition, BAN logic is employed to show the completeness of the scheme. After experimenting the proposed scheme, we observed that the less overheads are incurred in terms of costs required for communication and computation related to existing schemes. Lastly, we conclude that our client authentication scheme is offering more features than existing sachems.

Acknowledgements Supported by Visvesvaraya PhD Scheme, MeitY, Govt. of India. No. MEITY-PHD-3039.

Compliance with ethical standards

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

Human and animal rights The paper does not contain any studies with human participants or animals performed by any of the authors.

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

References

1. Sood SK, Sarjee AK, Singh K (2010) Anjour improvement of Liao et al.'s authentication scheme using smart card. In: 2010 IEEE 2nd International Advance Computing Conference (IACC2010), pp 240–245
2. He D, Kumar N, Chilamkurti N, Lee JH (2014) Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol. J Med Syst 38(10):1–6
3. Hwang MS, Li LH (2000) A new remote user authentication scheme using smart cards. IEEE Trans Consum Electron 46(1):28–30
4. Lee TF, Chang JB, Chan CW, Liu HC (2010) Password-based mutual authentication scheme using smart cards. In: The E-learning and Information Technology Symposium (EITS 2010)
5. Li CT, Lee CC, Weng CY (2014) A secure chaotic maps and smart cards based password authentication and key agreement scheme with user anonymity for telecaremedicine information systems. J Med Syst 38(9):77
6. He D, Kumar N, Chilamkurti N (2015) A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks. Inf Sci. https://doi.org/10.1016/j.ins.2015.02.010
7. He D, Zeadally S (2015) Authentication protocol for ambient assisted living system. IEEE Commun Mag 35(1):71–77
8. Chen CL, Yang TT, Chiang ML, Shih TF (2014) A privacy authentication scheme based on cloud for medical environment. J Med Syst 38(11):143
9. Wu ZY, Lee YC, Lai F, Lee HC, Chung Y (2012) A secure authentication scheme for telecare medicine information systems. J Med Syst 36(3):1529–1535
10. He DB, Chen JH, Zhang R (2012) A more secure authentication scheme for telecare medicine information systems. J Med Syst 36:1989–1995
11. Chen C, He D, Chan S, Bu SJ, Gao Y, Fan R (2011) Lightweight and provably secure user authentication with anonymity for the global mobility network. Int J Commun Syst 24(3):347–362
12. Lin HY (2013) On the security of adynamic ID-based authentication scheme for telecaremedical information systems. J Med Syst 37:9929
13. Cao T, Zhai J (2013) Improved dynamic ID-based authentication scheme for telecare medical information systems. J Med Syst 37:9912
14. Khan MK, Kumari S (2014) Cryptanalysis and improvement of "An efficient and secure dynamic ID-based authentication scheme for telecare medical information systems." Secur Commun Netw 7(2):399–408
15. Lee T-F, Chang I-P, Lin T-H, Wang C-C (2013) A secure and efficient password-based user authentication scheme using smart cards for the integrated EPR information system. J Med Syst 37(3):9941
16. Wen F (2014) A more secure anonymous user authentication scheme for the integrated EPR information system. J Med Syst 38(5):42
17. Das A (2015) A secure and robust password-based remote user authentication scheme using smart cards for the integrated EPR information system. J Med Syst 39:25
18. He D, Zeadally S (2015) An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. IEEE Internet Things J 2(1):72–83
19. 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
20. Abdellaoui A, Khamlichi YI, Chaoui H (2016) A robust authentication scheme for telecare medicine information system. Proc Comput Sci 98:584–589
21. Chaudhry SA, Mahmood K, Naqvi H, Khan MK (2015) An improved and secure biometric authentication scheme for telecare medicine information systems based on elliptic curve cryptography. J Med Syst 39:175. https://doi.org/10.1007/s10916-015-0335-y
22. Chaudhry SA, Khan MT, Khan MK, Shon T (2016) A multiserver biometric authentication scheme for TMIS using elliptic curve cryptography. J Med Syst 40:230. https://doi.org/10.1007/s10916-016-0592-4

23. Chaudhry SA, Naqvi H, Khan MK (2018) An enhanced lightweight anonymous biometric based authentication scheme for TMIS. Multimed Tools Appl 77:5503–5524. https://doi.org/10.1007/s11042-017-4464-9
24. Sutrala AK, Das AK, Odelu V, Wazid M, Kumari S (2016) Secure anonymity-preserving password-based user authentication and session key agreement scheme for telecare medicine information systems. Comput Methods Prog Biomed 135:167–185
25. Liu W, Xie Qi, Wang S, Bin Hu (2016) An improved authenticated key agreement protocol for telecare medicine information system. Springer Plus 5:555. https://doi.org/10.1186/s40064-016-2018-7
26. Masdari M, Ahmadzadeh S (2017) A survey and taxonomy of the authentication schemes in telecare medicine information systems. J Netw Comput Appl 87:1–19
27. Fan Wu, Li X, Sangaiah AK, Lili Xu, Kumari S, Liuxi Wu, Shen J (2018) A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. Future Gener Comput Syst 82:727–737
28. Li X, Niub J, Kumaric S, Wud F, Chooe K-K (2018) A robust biometrics based three-factor authentication scheme for global mobility networks in smart city. Future Gener Comput Syst 83:607–618
29. Chandrakar P, Om H (2017) A secure and robust anonymous three-factor remote user authentication scheme for multi-server environment using ECC. Comput Commun. https://doi.org/10.1016/j.comcom.2017.05.009
30. Hafizul Islam SK, Obaidat MS, Vijayakumar P, Abdulhay E, Fagen Li M, Reddy KC (2018) A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs. Future Gener Comput Syst 84:216–227
31. Cui J, Zhang J, Zhong H, Shi R, Yan Xu (2018) An efficient certificate less aggregate signature without pairings for vehicular ad hoc networks. Inf Sci. https://doi.org/10.1016/j.ins.2018.03.060
32. Jiang Qi, Ma J, Yang C, Ma X, Shen J, Chaudhry SA (2017) Efficient end-to-end authentication protocol for wearable health monitoring systems. Comput Electr Eng 63:182–195
33. Challa S, Das AK, Gope P, Kumar N, Wu F, Vasilakos AV (2018) Design and analysis of authenticated key agreement scheme in cloud-assisted cyber-physical systems. Future Gener Comput Syst. https://doi.org/10.1016/j.future.2018.04.019
34. Ostad-Sharif A, Abbasinezhad-Mood D, Nikooghadam M (2019) Efficient utilization of elliptic curve cryptography in design of a three-factor authentication protocol for satellite communications. Comput Commun 147:85–97
35. Wei J, Liu W, Hu X (2018) On the security and improvement of privacy-preserving 3-factor authentication scheme for TMIS. Int J Commun Syst. e3767
36. Chandrakar P, Om H (2018) An extended ECC-based anonymity-preserving 3-factor remote authentication scheme usable in TMIS. Int J Commun Syst e3540
37. Radhakrishnan N, Karuppiah M (2018) An efficient and secure remote user mutual authentication scheme using smart cards for Telecare medical information systems. Inform Med Unlocked. https://doi.org/10.1016/j.imu.2018.02.003
38. Alzahrani BA, Irshad A (2018) A secure and efficient TMIS-based authentication scheme improved against Zhang et al'.s scheme. Arab J Sci Eng 43:8239–8253. https://doi.org/10.1007/s13369-018-3494-6
39. Zhang LP, Zhu SH (2015) Robust ECC-based authenticated key agreement scheme with privacy protection for telecare medicine information systems. J Med Syst 39(5):1–13
40. Soni P, Pal AK, Hafizul Islam SK (2019) An improved three-factor authentication scheme for patient monitoring using WSN in remote health-care system. Comput Methods Progr Biomed 182:105054
41. Renuka KM, Kumari S, Li S (2019) Design of a secure three-factor authentication scheme for smart healthcare. J Med Syst 43:133. https://doi.org/10.1007/s10916-019-1251-3
42. Qiao H, Dong X, Shen Y (2019) Authenticated key agreement scheme with strong anonymity for multi-server environment in TMIS. J Med Syst 43:321. https://doi.org/10.1007/s10916-019-1442-y
43. Ostad-Sharif A, Abbasinezhad-Mood D, Nikooghadam M (2019) An enhanced anonymous and unlinkable user authentication and key agreement protocol for TMIS by utilization of ECC. Int J Commun Syst 2019:e3913. https://doi.org/10.1002/dac.3913
44. Dharminder D, Mishra D, Li X (2020) Construction of RSA-based authentication scheme in authorized access to healthcare services. J Med Syst 44:6. https://doi.org/10.1007/s10916-019-1471-6
45. Lo J-W, Chun-Yueh Wu, Chiou S-F (2020) A lightweight authentication and key agreement scheme for telecare medicine information system. J Internet Technol 21(1):263–272
46. Arshad H, Rasoolzadegan A (2016) Design of a secure authentication and key agreement scheme preserving user privacy usable in telecare medicine information systems. J Med Syst 40:237

47. Liu W, Liu J, Wu Q, Qin B, Naccache D, Ferradi H (2018) Efficient subtree-based encryption for fuzzy-entity data sharing. Soft Comput 22(23):7961–7976
48. 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(1):80063–80073
49. Meshram C, Lee CC, Ranadive AS, Li CT, Meshram SG, Tembhurne JV (2020) A subtree-based transformation model for cryptosystem using chaotic maps under cloud computing environment for fuzzy user data sharing. Int J Commun Syst 33(7):e4307
50. Meshram C, Lee CC, Meshram SG, Khan MK (2019) An identity-based encryption technique using subtree for fuzzy user data sharing under cloud computing environment. Soft Comput 23(24):13127–13138
51. Xiao D, Liao X, Deng S (2005) One-way hash function construction based on the chaotic map with changeable-parameter. Chaos Solitons Fract 241:65–71
52. Das AK, Goswami A (2014) An enhanced biometric authentication scheme for telecare medicine information systems with nonce using chaotic hash function. J Med Syst 38:27
53. 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
54. Witteman M (2002) Advances in smartcard security. Inf Secur Bull 7:11–22
55. Burrows M, Abadi M, Needham R (1990) A logic of authentication. ACM Trans Comput Syst 8(1):18–36
56. Sarkar P (2010) A simple and generic construction of authenticated encryption with associated data. ACM Trans Inf Syst Secur 13(4):33
57. Chang YF, Yu SH, Shiao DR (2013) An uniqueness-andanonymitypreserving remote user authentication scheme for connected health care. J Med Syst 37:9902
58. Li CT, Lee CC, Weng CY, Fan CI (2013) An extended multi-server-based user authentication and key agreement scheme with user anonymity. KSII Trans Int Inform Syst 7:119–131
59. Li CT (2013) A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card. IET Inform Secur 7:3–10
60. Shin-Yan C, Ying Z, Liu J (2016) Improvement of a privacy authentication scheme based on cloud for medical environment. J Med Syst 40:101
61. Niloofar R, Nazari M (2018) An efficient improvement remote user mutual authentication and session key agreement scheme for E-health care systems. Multimed Tools Appl 77:55–88
62. Arezou O-S, Abbasinezhad-Mood D, Nikooghadam M (2019) An enhanced anonymous and unlinkable user authentication and key agreement protocol for TMIS by utilization of ECC. Int J Commun Syst 32:e3913
63. He D, Kumar N, Lee JH, Sherratt RS (2014) Enhanced three-factor security protocol for consumer USB mass storage devices. IEEE Trans Consum Electron 60(1):30–37

Authors and Affiliations

Vishesh P. Gaikwad[1] · Jitendra V. Tembhurne[1] · Chandrashekhar Meshram[2] · Cheng-Chi Lee[3,4]

Vishesh P. Gaikwad
gaikwad.vishesh@cse.iiitn.ac.in

Jitendra V. Tembhurne
jtembhurne@iiitn.ac.in

Chandrashekhar Meshram
cs_meshram@rediffmail.com

[1] Department of Computer Science and Engineering, Indian Institute of Information Technology, Nagpur, India

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

[3] Department of Library and Information Science, Research and Development Center for Physical Education, Health, and Information Technology, Fu Jen Catholic University, New Taipei 24205, Taiwan, ROC

[4] Department of Photonics and Communication Engineering, Asia University, Wufeng Shiang, Taichung 413, Taiwan, ROC