A construction of a conformal Chebyshev chaotic map based authentication protocol for healthcare telemedicine services

Dharminder Dharminder · Uddeshaya Kumar · Pratik Gupta

Abstract
The outbreak of coronavirus has caused widespread global havoc, and the implementation of lockdown to contain the spread of the virus has caused increased levels of online healthcare services. Upgraded network technology gives birth to a new interface “telecare medicine information systems” in short TMIS. In this system, a user from a remote area and a server located at the hospital can establish a connection to share the necessary information between them. But, it is very clear that all the information is always being transmitted over a public channel. Chaotic map possesses a dynamic structure and it plays a very important role in the construction of a secure and efficient authentication protocols, but they are generally found vulnerable to identity-guess, password-guess, impersonation, and stolen smart-card. We have analyzed (Li et al. in Fut Gen Comput Syst 840:149–159, 2018; Madhusudhan and Nayak Chaitanya in A robust authentication scheme for telecare medical information systems, 2008; Zhang et al in Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme, 2017; Dharminder and Gupta in Pratik security analysis and application of Chebyshev Chaotic map in the authentication protocols, 2019) and found that Bergamo’s attack (IEEE Trans Circ Syst 52(7):1382–1393, 2005) cannot be resisted by the protocol. Although few of the protocols ensures efficient computations but they cannot ensure an anonymous and secure communication. Therefore, we have proposed a secure and efficient chaotic map based authentication protocol that can be used in telecare medicine information system. This protocol supports verified session keys with only two messages of exchange. Moreover, we have analysed the performance of proposed protocol with relevant protocols and it is being implemented in “Automated Validation of Internet Security Protocols and Applications” respectively.

Keywords Authentication · Security · Privacy · Key agreement · Chaotic mapping

Introduction
The adoption of advanced health care “Telemedicine Information System” and “Telematics” applications in health care needs an integrated strategy to the different social, financial, cultural and political impacts and hurdles of information and communication technologies. Both security and privacy [37–39,42] are two important attributes required to construct a secure authentication protocol. Security and privacy of “Telemedicine Information System” are the impressive components that are of great interest to the field of health care. Because the Internet is truly an open network with many potential security gaps, close consideration and measures must be required to ensure safe medical facilities and the safety of patient data. Both health care and treatment are two very important factors in the human’s life (see data in Fig. 1).

Upgraded technology in the field of online health care services such as variety of medical sensors, smart phones, and smart robotics helps the patients to facilitate the health care services in the remote areas. In these days, most of the doctors are employing robots and smart digital sensor in surgeries is an application of computer science in health care services [40,41]. There are other applications such as artificial intelligence and machine learning are used to detect the medical conditions of a patient. Nowadays, a patient possessing smart
sensors and mobile phones can enjoy benefits of health care services around the world (see Fig. 2).

Patients can be benefited with online health care services via their smart phones, i-pads, and other smart sensors, but their security and privacy are two very important components during communication on public channel. In 2012, Wu et al. [10] designed a secure and anonymous authentication protocol to benefit the patients at their home. In the same year, Wei et al. [9] analyses the security of the protocol [10] and it is found vulnerable to two-factor authentication. In order to eradicate the two-factor authentication defect, a fresh design is needed for two-factor authentication. In the same year, Zhu [12] discussed the security attributes such as password guessing in the protocol [9] and invented a password-guess resistant protocol, although he didn’t seem to think about communicating anonymously. In 2012, Chen et al. [4] designed an efficient and secure lightweight authentication protocol that preserves an anonymous communication in health care telemedicine services.

In 2013, Lin et al. [7] observed that identity can traced in [4] using both dictionary and password guess along with stolen smart card information. He tried to remove most of the existing attacks and he invented an anonymous authentication protocol. In the same year, Cao and Zhai [3] discussed both security and privacy of [4] and they found that the protocol is vulnerable against both identity guess and password guess along with the information stored in the smart card. Three protocols discussed [3,7,12] are found insecure to input ver-
ification procedure due to which they cannot differentiate incorrect inputs with in short time interval. The anonymous communication is another important factor that is missing in [9,10,12,32] respectively. In 2013, Guo et al. [14] used the complex dynamic structure of chaotic maps to design a new secure authentication protocol, but Hao et al. [15] discussed the security of the protocol and he found that two important attributes traceability and anonymity are missing, and he tried to fill the gap with a new design [14]. In 2014, Jiang et al. [16] reviewed both security and privacy attributes in [15] and he found the protocol is vulnerable to stolen smart card attack.

In the year 2016, Li et al. [21] designed a secure and efficient chaotic map-based authentication protocol to secure the communication in health care services, but in the year 2018, Madhusudhan et al. [20] discussed the attacks in [21] such as password guess, and impersonations, and he tried to remove these attacks as discussed in [20]. In the year 2018, Jiang et al. [28] introduced a secure and efficient protocol to improve the telemedicine services in health care sector, but it is not much efficient and it requires to exchange three messages to establish secure and fresh session key. In the same year 2018, Wu et al. [29] introduced a secure and efficient authentication protocol based on RFID and Radhakrishnan et al. [19] also proposed a new design to secure the health care telemedicine services, but their protocols found susceptible to password guess, identity guess and also for stolen card information too. In the same year 2018, Zhang et al. [25] introduced a lightweight and secure authentication protocol for the mobile devices used in health care telemedicine services, but it is also susceptible to identity guess, password guess and replay attacks. In 2018, Madhusudhan et al. [20] designed an efficient, and secure, and robust protocol for telecare services, but Dharminder et al. [35] discussed the security of the protocol [20] and they found it susceptible to identity guess, password guess, impersonations, and stolen smart card. In the same year 2020, Dharminder et al. [34] introduced a new design for authentication scheme based on RSA, but it uses the modulo operations that decreases the efficiency of the protocol due to costly modulo exponentiation.

In the Table 2, we have observed various security attributes achieved by the existing relevant chaotic map based authentication protocols used to secure TMIS system, where the symbol √ denotes “yes”, and × denotes “not” respectively. In the Tables 1, 2 one can see that existing protocols in the TMIS environment suffers various vulnerabilities such as password-guess, identity-guess, impersonations, replaying of older messages, and stolen smart card attacks. In the proposed design, we have discussed two important components security and privacy in the form of security attributes such as identity guess, impersonations, password guess, anonymity, replaying of messages, and stolen smart card information in the protocols [1,20,25,35] respectively. In the design [35], we have analyzed that a user $U_i$ selects $ID_i$, $PW_i$ and calculates $A_i = h(ID_i || PW_i)$, then he sends $< ID_i, A_i >$ to the server. Next, the server chooses a random $n_i \in Z_p^*$, and does the computation $B_i = T_s(ID_i || n_i) \oplus A_i$, it sends $< h(.), B_i, n_i >$ to the corresponding user. Now, the user $U_i$ calculates $B_i \oplus A_i = T_s(ID_i || n_i)$ then $D_i = h(T_s(ID_i || n_i) || PW_i || ID_i)$ and $N_i = n_i \oplus A_i$, and then store $B_i, D_i, N_i$ in the corresponding smart card. We have observed that a user knows $n_i \in Z_p^*$, and $T_s(ID_i || n_i)$ can executes Bergamo’s attack and computes $x'$ as $T_{v'}(ID_i || n_i) = T_s(ID_i || n_i)$ and uses $x'$ in the ongoing communication on the open channel.

Similarly, in the design [1], we have analyzed a vulnerability in the session key established during the communication. In the design [1], an adversary $A$ obtains the information from earlier transmitted information $M_1$ and $M_2$. Moreover, $A$ computes $u'$ with knowledge of $x$, $T_v(x)$ satisfying $T_v(x) = T_{v'}(x)$. Finally, $A$ guesses $u'$ under the previous knowledge $x$, $T_v(x)$ satisfies $T_v(x) = T_{v'}(x)$ as:

$$u' = \frac{arccos(T_u(x)) + 2k\pi}{arccos(x)}$$

$$v' = \frac{arccos(T_v(x)) + 2k\pi}{arccos(x)}$$

Where $k$ is a positive integer, finally $A$ finds $T_v(T_v(x)) = T_v(x)$, $T_v(x) = Sk_u = Sk_s$ that plays the role of session key.

Similarly, in the design [25], we have analyzed a vulnerability in the session key established during the communication. In the design [25], an adversary $A$ obtains the information from earlier transmitted messages $\{a_i, T_u(x), N_i d_i\}$, $\{b_i, T_v(x), m\}$ and $\{Y_i, N_i d_i, Z_i, h(.), V_i, x\}$ stored in the corresponding smart card. Further, $A$ obtains $u'$ under the knowledge of $x$, $T_u(x)$ satisfies $T_u(x) = T_{u'}(x)$. Further, $A$ makes a guess $s'$ under the knowledge of $x$, $T_v(x)$ satisfies $T_v(x) = T_{v'}(x)$.

$$u' = \frac{arccos(T_u(x)) + 2k\pi}{arccos(x)}$$

$$s' = \frac{arccos(T_v(x)) + 2k\pi}{arccos(x)}$$

Where $k$ is a positive integer, then $A$ computes $T_v(T_v(x)) = T_v(T_v(x)) = Sk_u = Sk_s$ that plays the role of session key during communication.

Similarly, in the design [20], we have analyzed a vulnerability in the session key established during the communication. In the design [20], an adversary $A$ obtains the information from earlier transmitted messages $\{C_i d_i, E_i, D_i, F_i\}$, $\{H_i, T_s(ID_i || n_i)\}$ and $\{B_i, h(.), C_i, n_i, D_i\}$ that is stored in the smart card. Further, $A$ computes $y'$ under the knowledge $ID_i, n_i, T_v(ID_i || n_i)$ satisfies $T_v(ID_i || n_i) = T_{v'}(ID_i || n_i)$. Further, $A$ makes a guess $z'$ under the knowledge $ID_i, n_i, T_v(ID_i || n_i)$ satisfies $T_v(ID_i || n_i) = T_{v'}(ID_i || n_i)$ as:
### Table 1  A review on security attributes of authentication protocols based on password for TMIS

| Security parameters\protocols | [3] | [4] | [11] | [7] | [30] | [24] | [13] | [31] |
|------------------------------|-----|-----|------|-----|------|------|------|------|
| Anonymity                    | √   | √   | √    | √   | √    | √    | √    | ×    |
| Password-guess               | ×   | ×   | ×    | √   | ×    | ×    | ×    | ×    |
| Session-key verification     | √   | ×   | ×    | ×   | √    | ×    | ×    | ×    |
| Impersonations               | √   | ×   | √    | ×   | ×    | √    | ×    | ×    |
| Replay-messages              | ×   | √   | √    | √   | √    | √    | √    | √    |
| Key-agreement                | √   | √   | ×    | √   | √    | √    | √    | √    |
| Stolen-card                  | √   | √   | √    | √   | √    | √    | √    | √    |
| Password-change              | √   | √   | √    | √   | ×    | ×    | √    | ×    |

### Table 2  A review of security attributes of authentication protocols based on chaotic map for TMIS

| Security parameters\protocols | [24] | [15] | [22] | [23] | [19] | [25] | [21] | [20] |
|------------------------------|-----|-----|------|-----|------|------|------|------|
| Anonymity                    | √   | √   | ×    | √   | √    | √    | ×    | ×    |
| Insider-security             | √   | √   | √    | √   | √    | √    | √    | √    |
| Password-guess               | √   | √   | √    | √   | ×    | ×    | ×    | ×    |
| Stolen-cards                 | √   | √   | √    | √   | ×    | √    | ×    | ×    |
| User’s impersonations        | √   | √   | √    | √   | √    | ×    | ×    | x    |
| Key-agreement                | √   | √   | √    | √   | √    | √    | √    | √    |
| Server’s impersonations      | √   | √   | √    | √   | √    | ×    | √    | x    |
| Replay-messages              | √   | √   | √    | √   | ×    | √    | √    | √    |
| Key-agreement                | √   | √   | √    | √   | √    | √    | √    | √    |
| Key-verification             | √   | ×   | √    | √   | √    | √    | √    | √    |

\[ y' = \arccos(T_u(ID_i || n_i)) + 2k\pi \]
\[ z' = \arccos(T_s(ID_i || n_i)) + 2k\pi \]

Where \( k \) is a positive integer, then \( A \) computes \( T_s T_u(ID_i || n_i) \)

\( = T_s T_u(|ID_i||n_i|) \) and \( S_{ki} = S_{kj} = h(h(ID_i)||T_s'(ID_i||n_i))||T_s'(ID_i||n_i)) \) that plays the role of session key during communication.

To handle the issues in [1,20,25,35], we have an idea to compute \( x = h(ID_i||s) \), where \( ID_i \) is the identity of \( i^{th} \) user and “s” is the long term secret key of the server, in this way a user possesses \( x \) that results from different \( ID_i \) concatenated with master key of the server to produce different secret keys \( x \) for each of the user. Now, the \( x \) will play the role in place of master secret that is different for each of the user. Therefore, we have designed a new authentication protocol possessing both security and efficiency using the dynamic Chaos theory.

The security of the presented scheme have been analyzed in random Oracle with this we also use the tool for authentication called “Automated Validation of Internet Security Protocols and Applications” respectively. Moreover, the presented protocol resists session key violation problem, that is proposed by Bergamo et al. [33] and establishes a session key with just two messages of exchange.

### Preliminaries

In this section, we will discuss some of the basic notations, terminologies and basic properties of conformal Chaos maps used in the proposed protocol. A conformal map is an angle-preserving transformation that preserves local angles. A brief review of some of the useful notations are also given in Table 3.
A review of dynamic structure of Chebyshev polynomials

Chebyshev chaotic mapping

As seen in Fig. 3, chaotic maps have a complex dynamic structure and it is well known for its pseudo randomness. In this subsection, we have discussed some of basic definitions and dynamic properties [17].

Definition 1 A polynomial \( T_v(y) : (-\infty, +\infty) \to [-1, +1] \) is introduced by Chebyshev in variable “\( y \)” and of positive degree \( v \), besides that \( T_v(y) = \cos(v \arccos(y)) \) and the recurrence \( T_v(y) \) is described as \( T_v(y) = 2yT_{v-1}(y) - T_{v-2}(y) \), whereas \( y \in (-\infty, +\infty) \) and \( T_0(y) = 1, T_1(y) = y \).

Theorem 1 The set of Chebyshev polynomials on \( R = (-\infty, +\infty) \) satisfies semigroup property under composition of chaotic maps.

Proof Chebyshev polynomials given in variable \( x \) is \( T_v(y) : (-\infty, +\infty) \to [-1, +1] \), where \( v > 0 \) is an integer, and \( T_v(y) = \cos(v \arccos(y)) \) under recurrence relation \( T_v(y) = 2yT_{v-1}(y) - T_{v-2}(y) \), furthers \( y \in (-\infty, +\infty) \) and \( T_0(y) = 1, T_1(y) = y \). Therefore, we get difference equation along with characteristics equation \( \rho^2 - 2y\rho + 1 = 0 \). Therefore, \( \rho_1 = y + \sqrt{y^2 - 1} \) and \( \rho_2 = y - \sqrt{y^2 - 1} \) are two characteristics roots of equation \( \rho^2 - 2y\rho + 1 = 0 \) along with \( \rho_1 + \rho_2 = 2y \) and \( \rho_1\rho_2 = 1 \). Therefore,

\[
T_n(y) = \frac{\rho_1^n + \rho_2^n}{2} = \frac{(y + \sqrt{y^2 - 1})^n + (y - \sqrt{y^2 - 1})^n}{2} = \sum_{i=0}^{\left\lfloor \frac{n}{2} \right\rfloor} C_n^i y^{n-2i} (y^2 - 1)^i
\]

Where \( n, i \) are positive integers and \( C_n^i = \frac{n!}{i!(n-i)!} \). Furthers, \( T_n(T_n(y)) = \frac{\xi_1^n + \xi_2^n}{2} \) where \( n_1, n_2 \) are positive integers and \( \xi_1 + \xi_2 = 2T_{n_2}(y) \), and \( \xi_1\xi_2 = 1 \). Therefore, \( \xi_1 + \xi_2^{-1} = \rho_1^n + \rho_1^{-n_2} \) then \( \xi_1 = \rho_1^{n_2} \) or \( \xi_1 = \rho_1^{-n_2} \). Furthermore, \( T_n(y) = \frac{\rho_1^n + \rho_2^n}{2} \) gives us \( T_{n_1n_2}(y) = \frac{\rho_1^{n_1n_2} + \rho_1^{-n_1n_2}}{2} \). Hence \( T_{n_1n_2}(y) = T_{n_1}(T_{n_2}(y)) = T_{n_2}(T_{n_1}(y)) = T_{n_1n_2}(y) \). □

Definition 2 If it is asked to find \( u \) such that \( T_u(x) = y \), where the values \( y \) and \( x \) are known to the adversary. Then this problem is known as Discrete Logarithm Problem (DLP).

Definition 3 Computational Diffie-Hellman Problem (CDHP) can be stated to find \( T_{uv}(x) \), where the values \( x, T_u(x) \) and \( T_v(x) \) are known to the adversary.

Fuzzy extractor

A fuzzy extractor \( (E_f, R_f) \) [2] is an extraction mechanism that is used to extract a random uniform string from biometric imprints \( bm_i \). It consists of two algorithms \( I(.) \) and \( R(.) \). \( I(.) \) is a probabilistic algorithm that produced two strings \( b_1, b_2 \) as output after taking \( bm_i \) an input parameter, where \( b_1 \) is private key and \( b_2 \) is a helper string. \( R(.) \) is an algorithm that is used to regenerate the private key \( b_1 \) after taking noisy biometric parameter \( bm_i \) and helper string \( b_2 \) as input, where \( |bm_i - bm_i'| \leq \delta \).

Proposed authentication protocol under chaotic mapping

We have proposed a secure and efficient chaotic map based authentication that can be divided into four phases, (1) registration-phase, (2) login-phase, (3) authentication-phase and (4) password-update-phase.

Registration-phase

\( U_i \) registers to the concern server \( S r_j \) via a secure channel as written in the following lines.

- \( U_i \) selects \( ID_i, P s_i \), and imprints his own biometric \( bm_i \) then compute \( I(bm_i) = (b_1, b_2) \), \( U_i = h(I(D_i)||P s_i||b_1) \) and transmits \( ID_i, U_i \) to \( S r_j \).
- After getting the information \( \{ ID_i, U_i \} \), \( S r_j \) chooses arbitrary \( p_i \in Z_p^* \), then compute first \( x = h(ID_i||s) \), where “\( s \)” is the private key of \( S r_j \). Now, it computes \( S i_1 = T_1(ID_i), S i_2 = T_1(ID||p_i) \). Then, it calculates the value \( S i_3 = (S i_1||S i_2) \oplus U_i \) and store \( h(.) \), \( S i_3 \), \( p_i \).
- \( S r_j \) delivers a hidden information \( \{ h(.) \} \), \( S i_3 \), \( p_i \), after stored it into the smart-card, to \( U_i \) via a private channel.
- Finally, \( U_i \) does the computations \( S i_1||S i_2 = S i_3 \oplus U_i \), \( U_i = h(S i_1||S i_2||P s_i||I(D_i)||b_1), P_i = p_i \oplus U_i \) and store \( \{ h(.) \}, S i_3, U_i, P_i, b_2 \) into the smart card.
Fig. 4 A description of registration phase via secure channel

\[ U_i \text{ selects } ID_i, \ P_{si}, \ \text{and imprint } bm_i \]
Computes
\[ I(bm_i) = (b_1, b_2) \]
\[ U_{i1} = h(ID_i||P_{si}||b_1) \]

\[ < ID_i, U_{i1} > \]
choose random \( p_i \in Z_p^* \)
Computes
\[ x = h(ID_i||s) \]
\[ S_{i1} = T_x(ID_i) \]
\[ S_{i2} = T_x(ID_i||p_i) \]
\[ S_{i3} = (S_{i1}||S_{i2}) \oplus U_{i1} \]

\[ < h(\cdot), S_{i1}, p_i > \]

Fig. 5 A description of login and authentication phases

**Login phase**

If \( U_i \) wants to login to \( Sr_j \) then:

- \( U_i \) firstly insert the card into card reader machine, then input \( ID_i, P_{si} \) and imprints the biometric \( bm_i \), then the card computes \( I(bm_i) = (b_1, b_2) \) and \( U_{i1} = h(ID_i||P_{si}||b_1) \).
- Using \( U_{i1} \) the smart card executes the step \( S_{i1} = S_{i1} \oplus U_{i1} \) and computes \( U_{i2} = h(S_{i1}||P_{si}||b_1) \) and proceeds for the legal verification \( U_{i2} = ?U_{i2} \).
- The choose \( y \in Z_p^* \) arbitrarily and further proceeds to compute
\[ U_{i3} = T_y(ID_i||p_i) \]
\[ U_{i4} = T_y(ID_i) \]
\[ S_{ki} = h(T_y(S_{i2}||T_1)) = h(T_y(ID_i||p_i)||T_1) \]
\[ U_{i5} = h(U_{i3}||U_{i4}||S_{ki}||T_1) \]
\[ NID_i = (U_{i3}||U_{i4}||ID_i) \oplus T_y(S_{i1}) = (U_{i3}||U_{i4}||ID_i) \oplus T_y(T_x(ID_i)) \] and then \( U_i \) transmits \( < U_{i4}, NID_i, T_1 > \) to \( Sr_j \).

**Authentication phase**

\( Sr_j \) receives \( < U_{i4}, NID_i, T_1 > \) from corresponding \( U_i \) and executes the process of authentication:

- \( Sr_j \) verifies the time stamp \( T_1 \), and computes \( T_x(U_{i4}) = T_x(T_y(ID_i)) \)
\( T_x(T_y(ID_i)) \oplus NID_i = ID_i \oplus U_{i3} \) \( U_{i2} \) then after getting \( ID_i \) \( Sr_j \) computes \( x'' = h(ID_i^3||s) \)
\( S_{ki}'' = h(T_x(U_{i3}^3)||T_1) = h(T_x(T_y^3(ID_i||p_i)||T_1) \) and then ver-
ifies $U_{i_3}' = ?U_{i_5}$ where $U_{i_3}' = h(U_{i_5}' || U_{i_4} || S_{i_3}' || T_1)$ finally $S_{i_4}$ computes $S_{i_4} = h(S_{i_3} || I_{D_1} || T_2)$.

- $S_{r_j}$ transmits the information $\{S_{i_4}, T_2\}$ to $U_i$ through public channel.
- After receiving the information $\{S_{i_4}, T_2\}$ from $S_{r_j}$, then $U_i$ confirms $T_2$ is valid or not, then he calculates $S_{i_4}' = h(S_{i_3} || I_{D_1} || T_2)$, and proceeds the verification $S_{i_4}' = S_{i_4}$, and establishes a session key $S_{k_i} = h(T_y, T_x, (I_{D_1} || p_j)) || T_1)$.

### Password update phase

To update password $U_i$, executes the following steps:

- $U_i$ inputs $I_{D_1}$ and $P_{s_i}$. Furthermore, he imprints biometric, then computes $I(b_{m_1}) = (b_1, b_2)$ and $U_{i_2}' = h(I_{D_1} || P_{s_i} || b_1)$, using $U_{i_2}'$, the $S_{c_i}$ obtains $S_{i_2}'$, $S_{i_2}' = S_{i_2} \oplus U_{i_2}'$, and $U_{i_2}' = h(S_{i_2}' || S_{i_3}' || P_{s_i} || I_{D_1} || b_1)$ and proceeds for the verification $U_{i_2}' = U_{i_2}$.

- $U_i$ inputs $P_{s_i}'$ new and proceeds the computation $U_{i_2}' = h(I_{D_1} || P_{s_i} \text{new} || b_1)$, $U_{i_2}' = h(S_{i_2}' || S_{i_3}' || P_{s_i} \text{new} || I_{D_1} || b_1)$, $S_{i_3}' = U_{i_2}' \oplus S_{i_2}'$, and updates the values $S_{i_3}, U_{i_2}$ with $S_{i_3}'$, $U_{i_2}'$.

### Security analysis

#### Formal security analysis

At first, we have to define a framework $\mathcal{P}$ to verify the security of the presented protocol and then, under random oracle, we will implement the presented protocol.

**Security-model** Suppose the $i^{th}$ instance of a user $U_i$ is denoted by $M_i \in (U_i, S_{r_j})$, and $A$ be an attacker that governs the connection between $U_i$ and $S_{r_j}$. An illustration of $A$, is therefore stated as follows:

- **Extract:** With the help of extract query, $A$ could get the private key of a user $U_i$.

- **Send** ($m, M_i$): With the help of send query, $A$ could be able to send arbitrary message $m$, to random oracle then in response of $m$, random oracle have to reply with a computational output.

- **Hash** ($m$): In this query $A$ sends random massage $m$ to $H(.)$, then oracle select $s \in Z_p$ randomly and reply with $s$, after storing it into hash list $H_{ij}$ with $m$. Initially $H_{ij}$ assumed to be empty.

- **Reveal** ($M_i$): If an adversary $A$ process a reveal query to oracle, then oracle permits $A$, to know about session key $S_{k_i}$.

- **Corrupt** ($M_i$): Corrupt query allows $A$ to obtains the private key of $M_i$, by corrupting $M_i$.

- **Test** ($M_i$): If oracle receives test query, oracle guesses a random bit $b \in \{0, 1\}$. Then two cases aries: (1) if $b = 0$, then oracle reply with arbitrary number, (2) if $b = 1$, then oracle reply with session key $S_{k_i}$.

Suppose a bit $b$ is selected from corrupt query phase and $Succ(A)$ correctly estimates the value of $b$, then the advantage $Adv_{A, p}(k)$, against the protocol retained by adversary is specified as:

$$Adv_{A, p}(k) = |2 \cdot Pr[Succ(A)] - 1|$$

**Mutual authentication** is established by security analysis in Random Oracle for the suggested scheme.

**Chaotic based assumption:** Suppose $x \in Z_p^*$ is a secret key of $S_{r_j}$, $p$ is a prime number with length $n$, then from generation algorithm $Gen(1^n) = p$.

$\exists$ a negligible function $neg(n)$ such that:

$$Pr(Gen(1^n) \rightarrow p, x, r, T_x(r) \leftarrow Z_p^*)$$

$\forall$ probabilistic polynomial time adversary $A$.

**Collision resistance attack(CRA) algorithm:** If for $h(.)$, $A$, then we have

$$Adv_A = Pr[(c, c') \leftarrow R : c \neq c' \text{and } h(c) = h(c')]$$

**Theorem 2** Suppose $\mathcal{R}$ be a RO and if $A$ breach the suggested mutual authentication protocol, then we can design an algorithm $M_O$, to solve CRA problem, together with $A$.

**Proof** At first, $M_o$ detects $U_{i_4}, NID_{i_1}, H_{i_1}$ and then to solve the problem of CRA, $M_o$ attempts to calculate $X_{i_1}$ and $r*$ and verifies $h(r* || P_{s_i} || I_{D_1} || H_{i_1}) = ?U_{i_5}$ or $U_{i_5} = ?h(U_{i_3} || U_{i_4} || S_{ki} || T_1)$. $M_o$ have access to $\mathcal{R}, , p, o, T, Gen(.)$, also $M_o$ can reach to $A$ through query.

**Hash query:** When $A$ asks hash query $H_q$, for $I_{D_1}, M_o$ first check $H_{ij}$ list for $I_{D_1}$. If $M_o$ found it in the list $H_{ij}$, then it reply $h_{ij}$, otherwise $M_o$ calculates $h_u = H_1(I_{D_1})$ and put it in the list along with $I_{D_1}$, and sends $h_u$ back to $A$.

**Extract:** In extract query $A$ sends query on $I_{D_1}$. After getting extract query $M_o$, checks $h_u \in \{H_1, U_{i_4}, NID_{i_1}\}$. If $M_o$ fails to verify, then $M_o$ ends the process. After this, $M_o$ searches $I_{D_1} \in H_{ij}$, if present, then it responds, else calculates $X_{i_1} = U_{i_4}$ and return $h(S_{i_2} || P_{s_i} || I_{D_1} || H_{i_1}) = U_{i_2}$ to $A$.

**Send-queries:** In send query there are three phases discussed as below, first $U_i$ request for login to $S_{r_j}$, then $U_i$ sends a message $< (U_{i_4}, NID_{i_1}, T_1) >$ to $S_{r_j}$, and at last $S_{r_j}$ responds $(S_{i_4}, T_3)$. We will describe this phase by a game between $U_i$ and $S_{r_j}$ respectively.

1. $A$ start it with sending a query, in response of that $M_o$ is supposed to reply a login message to $A$.
2. $A$ sends polynomial time send queries, to login into $Sr_j$, then $M_o$ computes corresponding to $i^{th}$ query as $U_{i4} = T_s(ID_i)$ and $U_{i2} = h(Si_2||P_{si}||ID_i||p_i)$ responds to $A$.

3. $A$ submits $(U_{i2}, U_i)$, then $M_o$ verifies first whether $h_u \in H_{ij}$ or not. If it is present, then $M_o$ returns a failure, else ends the query $Q_{ei}$. Further, $M_o$ computes $R_1 = T_y(ID_i||p_i)$, and $S_k = T_y(ID_i||p_i)$ for arbitrary $j, y$ and $E_i = h(T_y(ID_i||p_i)||S_k||T_y)$ and returns the output to $A$.

4. $A$ submits $((T_y(r_1),U_{i5}))$, then $M_o$ computes $S_i = h(ID||r)$ and $U_{i2} = h(ID||p_i)||P_{si}||ID_i||p_i)$, where $r$ is chosen arbitrarily, then check the equation $W_i = ?_h(T_y(r))||P_{si}||ID_i||p_i)$, if holds, then $M_o$ does the computation $S_k = T_y(T_y(ID_i||N_i))$, $S_i = h(S_k||T_y)$ responds $(S_i4, T_y)$ to $A$.

5. $A$ submits $((S_i4, T_y), U_i)$, then $M_o$ does computations discussed above and get $V_2$, then verify $S_i4 = ?_h(S_k||T_y)$ and at last authenticates $A$.

Analysis If $A$ violates the authentication process between $U_i$ and $Sr_j$, then without knowing about the private key, the authentication message $M_1 = T_y(Si_2)$ could be forged by $A$, $A$ can send a duplicate message $Si_2$.

If without any knowledge about privet key, $A$ is able to forge $M_1 = T_y(r_1)$, then it can sends a duplicate $Si_2$. If $M_1 = h(X) \in L_{ij}$, then failed to proceed $P_{c2}$. Else, $M_o$ solves the problem of $CRA$. As $H(ID_i) \notin L_{ij}$, $A = h(B) \notin (s_{i1}, s_{i2}, \ldots)$, let the chance of success of $M_o$ be $\alpha$, and the chance of violating the protocol be $\beta$ respectively. Then, if event $P_{c1}$, $P_{c1}$, $P_{c2}$ exist then hash query, extract query and send query are legal. So, to break $CRA$ problem $M_o$ takes the help of $A$, if none of $P_{c1}, P_{c1}, P_{c2}$ happened. Thus,

$$Pr[-P_{c} \land -P_{c1} \land -P_{c2}] = \left(\frac{p_q}{H_q}\right)^{p_q+S_q} \left(\frac{H_q - E_q}{H_q}\right)$$

Therefore, $M_o$ is successful with advantage

$$\alpha \geq \left(\beta - \frac{1}{2^n}\right) \left(\frac{p_q}{H_q}\right)^{p_q+S_q} \left(\frac{H_q - P_q}{H_q}\right)$$

So, we can observe that the algorithm $M_o$ has the advantage, so if $A$ can breach the scheme, then $M_o$ can breach the suggested protocol, using subroutine $A$.

**Theorem 3** The protocol is secured against chosen message attack in RO model, if Chaotic discrete logarithm problem (CDLP) holds.

**Proof** By contradiction, let us prove this, let us say that there is $A$, who breaches proposed scheme against chosen message attack, so we can model an algorithm $mo$ that violates the discrete logarithm presumption based on the Chaotic map (CDLP), which implies that $A$ breaches the proposed system, then $mo$ breaches the proposed system as well, which means $A$ breaches the proposed scheme with non-negligible advantage.

**Game 1:** Suppose that $A$ is playing a chosen massage attack game with the suggested scheme. At first, $A$ possesses security parameter $1^n$ and map $T$, then $A$ uses message space $M$, to send massages $(M_0, M_1)$, to perform encryption queries $Q_E$. After getting massage, oracle selects arbitrary $m \in \{0, 1\}$ and applies $E_1 = T_y(M_m)$ and selects $y \in \{0, 1\}$ computes $E_2 = y \oplus M_m$, then reply $E_m = (E_1, E_2)$. Finally, if $A$ guesses a correct bit $m'$, where $m = m'$ then $A$ wins the game.

**Game 2:** In this phase $M_o$ tries to breach the assumptions. Since CDLP says challenger can obtain $s, q \leftarrow Z_n$* by running $Gen(.)$ algorithm and returns $(1^n, T_y(s))$ to $M_o$. Now $M_o$ has to return $s$ without having $y$.

**Game 3:** To guess $y$ correctly, $A$ has three options:

1. If $T_y(T_y(r)) = T_y(T_y(r))$ implies $z' = z$, $A$ continues to oracle with a random $z$, then it calculates $C_1 = T_y(r)$, else $RO(z) = y$, and reports $y' = y$. However, $A$ have non negligible chance of conducting such a query, so $M_o$ will win with a non-negligible gain. However, it has been concluded that $M_o$ violates the assumption with a marginal chance that implies $A$ has a neg(n) gain.

2. In this case $A$ have no clue about $y$ because there is no query about $z$ following $T_y(T_y(r)) = T_y(T_y(r))$. Now since $C_2 = y \oplus M_y$ works as one time pad so the probability of winning of $A$ is $Pr[A : win] = \frac{1}{2}$.

3. So the probability of $A$ for winning the game is $Pr[A : win] = \frac{1}{2} + \text{neg}(n)$, that contradicts our assumption.

\[\square\]

**Informal security analysis**

**Anonymous**

If for any protocol, it is impossible for any adversary, to find user’s real identity then we says that protocol follows the anonymous property. In our protocol, user’s identity is not used over public channel, instead we use $NID_i = (U_{i3}||U_{i5}||ID_i) \oplus T_y(Si_1)$. Adversary can intercept $NID_i$ and $U_{i4}$ but it is not possible for adversary to extract $ID_i$ from $NID_i$ because for that $A$ needs to compute $T_y(U_{i4})$ that requires long term secret key $s$ of server.
Password guessing attack

Password guessing attack is not possible on proposed scheme because \( A \) needs \( Si_3, Ui_2, ID_i, Hi \) simultaneously to implement it successfully. Adversary might get \( Si_3, Ui_2 \) by side channel attack or by power analysis attack but then he also need \( ID_i \) and \( Hi \), which is not possible.

Privileged insider attack

Since in registration phase user \( U_i \) send \( ID_i, Ui_1 \) to the server \( Sr_j \), where \( UI_1 = h(ID_i \| P_{Si_1} \| H_i) \). So it is not possible for any insider to know the password and biometric of any user because these are protected by hash function \( h(.) \). It makes proposed scheme secure against privileged insider attack.

Impersonation attack

If \( A \) wants to act like a legitimate user, he needs to send \( NID_i \) correctly to the server, where \( NID_i = (U_i || Si_1 || ID_i) \oplus T_y(Si_1) = (U_i || Si_1 || ID_i) \oplus T_y(T_i(ID_i)) \). To create \( NID_i \), \( A \) needs \( Si_2 \), which is protected by \( UI_1 \) and \( UI_1 = h(ID_i \| P_{Si_1} \| H_i) \). So basically \( A \) needs \( ID_i, Ps_{i_1} \) and \( Hi \) to impersonate user.

Again if \( A \) wants to impersonate server then he need to create \( Si_4 \) correctly and for this \( A \) needs server’s long term secret key \( s \). So above discussion suggest that proposed scheme is secure against impersonation attack.

Reply attack

Since we use different random number \( y \) for every session in proposed scheme where session key depends upon \( y \), with this we also use time stamp, to avoid this type of attacks. For every session, the timestamp is uniquely chosen. The timestamp uniqueness property limits the duplication of login messages. This indicates that the proposed system is responsive to replay attacks.

Perfect forward secrecy

Even if long term secret key \( s \) is compromised, suggested scheme is secure. Because to create session key \( A \) needs to compute \( x \) and for this \( A \) need \( ID_i \) which is not possible because we do not send \( ID_i \) through public channel.

Man in the middle attack

If any adversary \( A \) wants to implement man in the middle attack then firstly \( A \), intercept the message \( Ui_4, NID_i, T_i \), where \( Ui_4 = T_y(ID_i) \) and \( NID_i = (U_i || Si_3 || ID_i) \oplus T_y(Si_3) = (U_i || Si_3 || ID_i) \oplus T_y(T_i(ID_i)) \). Since \( ID_i \) of \( U_i \) is hidden in \( NID_i \) and it is not practically possible for any adversary to extract \( ID_i \) from public channel information therefore adversary fails to forge \( Ui_4 \). So proposed scheme is secure against man in the middle attack.

Stolen card attack

If adversary get access to the smart card of a user and extract \( P_i, Si_3 \) and \( Ui_2 \) from smart card. Even then he could not able to get any meaningful information, that helps \( A \) to breach the security of proposed protocol because all of these are secured by hash function. \( A \) needs \( ID_i, Ps_{i_1} \) and \( Hi \) simultaneously get useful information which is not possible.

Simulation and output using “Automated Validation of Internet Security Protocols and Applications”

In this subsection, we simulate the scheme using “Automated Validation of Internet Security Protocols and Applications” in short AVISPA tool to analyse formal security (man in the middle attack, replay attack) [36]. We have provided essential illustration on the basic output in OFMC and ATSE modes in Fig. [6].

Performance analysis

In this section, we have analyzed the performance of the proposed protocol and the performance of the proposed protocol has been compared with the related chaotic map based authentication scheme in the Table 4, where the cost of various operations are \( h_i \approx 0.005s, s_i \approx 0.0087s, m_t \approx 0.06307s, \) and \( c_i \approx 0.02102s \) denote the time for hashing, message encryption under symmetric key, one ordinary multiplication in \( Z_p^* \) and chaotic based operation respectively.

We have analysed the performance of chaotic map based authentication protocols [1,15,16,20,22,24,25] with the proposed protocol. As we know our mobile phones has limited storage and random access memory, and internet connectivity is another problem, that all the telecare medicine services runs on limited bandwidth network that is why we need a secure and efficient authentication protocol. Both computation and communication efficiency are very important and these two costs of computations have been compared with existing protocols in the Table 4. The various operation cost estimated via executing an experiment on intel Pentiums-4 (1024 MB ram) processor as in [6,35] with this computation cost described in Fig. 7.

In addition, Liu et al. [22] runs with computation cost \( 4h_i + 2c_i \) at user side, \( 5h_i + 2c_i \) at server side, Jiang et al. [16], at user side runs with computation cost \( 2h_i + s_i + c_i \) at server side use \( 2h_i + 2s_i + 3c_i \), Hao et al. [15] at user side runs.
Fig. 6 Illustration of output of HLPSL code in OFMC and ATSE modes

Fig. 7 Computation cost comparison

Table 4 A performance analysis of the proposed protocol with recent chaotic map-based authentication protocols

| Schemes                  | User-computation | Server-computation | Messages |
|--------------------------|-------------------|--------------------|----------|
| Liu et al.’s [22]        | $4h_t + 2c_t$     | $5h_t + 2c_t$      | 3        |
| Jiang et al.’s [16]      | $2h_t + s_t + c_t$| $2h_t + 2s_t + 3c_t$| 2        |
| Hao et al.’s [15]        | $2c_t + 3h_t + 2s_t$| $2c_t + 3s_t + 2h_t$| 2        |
| Lee’s [24]               | $2c_t + 7h_t$     | $2c_t + 8h_t$      | 2        |
| Zhang et al.’s [25]      | $6h_t + 2c_t$     | $4h_t + 1c_t + 2s_t$| 3        |
| Madhusudhan et al.’s [20]| $7h_t + 2c_t$     | $3h_t + 2c_t$      | 2        |
| Li et al.’s [1]          | $7h_t + 2c_t$     | $7h_t + 2c_t$      | 2        |
| Proposed                 | $4c_t + 4h_t$     | $2c_t + 4h_t$      | 2        |
with computation cost $2c_t + 3h_t + 2s_t$, at sever computation cost is $2c_t + 3s_t + 2h_t$, Lee et al. [24], at the user side runs with computation cost $2c_t + 7h_t$, at the server side it takes $2c_t + 8h_t$, Zhang et al. [25] runs with computation cost $6h_t + 2c_t$ on the user side, and at server cost is $4h_t + 1c_t + 2s_t$, Madhusudhan et al. [20] at user side runs with computation cost $7h_t + 2c_t$, at server side $3h_t + 2c_t$, Li et al. [1] runs with computation cost $7h_t + 2c_t$ at the user side, and at server side cost is $7h_t + 2c_t$, whereas the suggested protocol runs with computation cost $4c_t + 4h_t$ at the user side, $2c_t + 4h_t$ at the server side respectively.

In this article, we have considered the cost of communication in the form of hashing, chaotic operation, and time-stamp as 160-bits, and symmetric encryption outputs standard 256 bits, whereas total cost of communication is given in the Fig. 8 and the cost of computation is shown in the Fig. 8.

### Conclusion

This article provides a review on the security of recently proposed chaotic map based authentication protocol. The suggested design is free from most of the existing vulnerabilities such as password-guess, identity-guess, impersonations, replaying of messages, and stolen smart cards attacks and it also gives the idea how a poor verification results vulnerabilities. Furthermore, we have observed that the proposed design fulfills the requirement of session key verification in just two message exchange. In future, we can implement the protocol in vehicular communications, and digital rights management system etc.

### Declarations

**Conflict of interests** All the authors have no conflict of interests.

**Research involving human participants/animals** Research does not involve any human participant and/or animal performed by any of the authors.

**Informed consent** All the authors have agreed to this submission.

**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

### References

1. Li X, Wu F, Khan MK, Xu L, Shen J, Jo M (2018) A secure chaotic map-based remote authentication scheme for telecare medicine information systems. Fut Gen Comput Syst 840:149–159
2. Dodis Y, Reyzin L, Smith A (2004) Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. Int Conf Theory Appl Cryptogr Tech 00:523–540
3. Cao T, Zhai J (2013) Improved dynamic id-based authentication scheme for telecare medical information systems. J Med Syst 37(2):1–7
4. Chen HM, Lo JW, Yeh CK (2012) An efficient and secure dynamic id-based authentication scheme for telecare medical information systems. J Med Syst 36(6):3907–3915

5. Avoine Gildas Adversarial (2005) Model for radio frequency identification IACR crypology. Arch Citeseer 1–49

6. Kocarev L, Lian S (2011) Chaos-based cryptography: theory, algorithms and applications. Springer, New York, pp 330–354

7. Lin HY (2013) On the security of a dynamic id-based authentication scheme for telecare medical information systems. J Med Syst 37(2):1–5

8. Dolev D, Yao A (1983) On the security of public key protocols. IEEE Trans Inf Theory IEEE, pp 198–208

9. Wei J, Hu X, Liu W (2012) An improved authentication scheme for telecare medicine information systems. J Med Syst 36(6):3597–3604

10. 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

11. Xie Q, Zhang J, Dong N (2013) Robust anonymous authentication scheme for telecare medical information systems. J Med Syst 37(2):1–8

12. Zhu Z (2012) An efficient authentication scheme for telecare medical information systems. J Med Syst 36(6):3833–3838

13. Jiang Q, Ma J, Ma Z, Li G (2013) A privacy enhanced authentication scheme for telecare medical information systems. J Med Syst 37(1):1–8

14. Guo C, Chang CC (2013) Chaotic maps-based password-authenticated key agreement using smart cards. Commun Nonlinear Sci Numer Simul 18(6):1433–1440

15. Hao X, Wang J, Yang Q, Yan X, Li P (2013) A chaotic map-based authentication scheme for telecare medical information systems. J Med Syst 37(2):1–7

16. Jiang Q, Ma J, Lu X, Tian Y (2014) Robust chaotic map-based authentication and key agreement scheme with strong anonymity for telecare medical information systems. J Med Syst 38(2):1–8

17. Kohda T, Tsuneda A, Lawrance AJ (2000) Correlational properties of chebyshev chaotic sequences. J Time Ser Anal 21(2):181–191

18. Kohda T, Tsuneda A (1993) Pseudonoise sequences by chaotic nonlinear maps and their correlation properties. IEICE Trans Commun 76(8):855–862

19. Radhakrishnan N, Karuppiah M (2018) An efficient and secure remote user mutual authentication scheme using smart cards for Telecare medical information systems. Inf Med Unlocked Year Elsevier, pp 1–38

20. Madhusudhan R, Nayak Chaitanya S (2018) A robust authentication scheme for telecare medical information systems. Multimed Tools Appl. Springer, New York, pp 1–19

21. Li C-T, Lee C-C, Weng C-Y, Chen S-J (2016) A secure dynamic identity and chaotic maps based user authentication and key agreement scheme for e-healthcare systems. J Med Syst Springer, New York, pp 11–233

22. Liu Y, Xue K (2016) An improved secure and efficient password and chaos-based two-party key agreement protocol. Nonlinear Dyn Springer New York, pp 549–557

23. Li C-T, Lee C-C, Weng C-Y (2014) A secure chaotic maps and smart cards based password authentication and key agreement scheme with user anonymity for telecare medicine information systems. J Med Syst Springer, New York, pp 9–86

24. Lee TF (2013) An efficient chaotic maps-based authentication and key agreement scheme using smartcards for telecare medicine information systems. J Med Syst 37(6):1–9

25. Zhang L, Zhu S, Tang S (2017) Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme. IEEE J Biomed Health Inf IEEE, pp 465–475

26. Amin R, Biswas GP (2015) An improved rsa based user authentication and session key agreement protocol usable in tmis. J Med Syst Springer, New York, pp 8–87

27. Burrows M, Abadi M, Needham RM (1989) A logic of authentication. Proc R Soc Lond A Math Phys Sci 426(1871):233–271

28. Jiang Q, Chen Z, Li B, Shen J, Yang L, Ma J (2018) Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems. J Ambient Intell Hum Comput Springer, New York, pp 1061–1073

29. Wu F, Xu L, Kumari S, Li X, Das AK, Shen J (2018) A lightweight and anonymous RFID tag authentication protocol with cloud assistance for e-healthcare applications. J Ambient Intell Hum Comput Springer, New York, pp 919–930

30. Xu X, Zhu P, Wen Q, Jin Z, Zhang H, He L (2014) A secure and efficient authentication and key agreement scheme based on ecc for telecare medical information systems. J Med Syst 38(1):1–7

31. Wu F, Xu L (2013) Security analysis and improvement of a privacy authentication scheme for telecare medical information systems. J Med Syst 37(4):1–9

32. Lee TF, Chang IP, Lin TH, Wang CC (2013) A secure and efficient password-based user authentication scheme using smart cards for the integrated EPR information system. J Med Syst 37(3):1–7

33. Bergamo P, D’Arco P, De Santis A, Kocarev L (2005) Security of public-key cryptosystems based on Chebyshev polynomials. IEEE Trans Circ Syst 52(7):1382–1393

34. Dharminder D, Mishra D, Li X (2020) Construction of RSA-based authentication scheme in authorized access to healthcare services. J Med Syst 44(1):1–6

35. Dharminder D, Gupta (2019) Pratik security analysis and application of Chebyshev Chaotic map in the authentication protocols. Int J Comput Appl 0(0):1–9

36. Armando A, Basin D, Boichut Y, Chevalier Y, Compagna L, Cuellar J, Drielsma PH, Heam P-C, Koucharenko O, Mantovani J (2005) The AVISPA tool for the automated validation of internet security protocols and applications. In: International conference on computer aided verification, pp 281–285

37. Song J, Zhong Q, Wang W, Su C, Tan Z (2020) FPDP: flexible privacy-preserving data publishing scheme for smart agriculture. IEEE Sens J

38. Wang W, Huang H, Zhang L, Su C (2020) Secure and efficient mutual authentication protocol for smart grid under blockchain. Peer–Peer Netw Appl 00:1–13

39. Javed AR, Beg MO, Asim M, Baker T, Al-Bayatti A (2020) Hilal AlphaLogger: Detecting motion-based side-channel attack using smartphone keystrokes. J Ambient Intell Hum Comput 00:1–14

40. Javed AR, Sarwar MU, Beg MO, Asim M, Baker T, Tawfik H (2020) A collaborative healthcare framework for shared healthcare plan with ambient intelligence human-centric computing and information sciences. J Ambient Intell Hum Comput 101:1–21

41. Sarwar MU, Javed AR (2019) Collaborative health care plan through crowdsource data using ambient application. In: 22nd International multtopic conference (INMIC), pp 1–6

42. Zhang L, Zou Y, Wang W, Jin Z, Su Y, Chen H (2021) Resource allocation and trust computing for blockchain-enabled edge computing system. Comput Secur 1050:102249

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