Malaya Journal of Matematik, Vol. 8, No. 4, 2127-2136, 2020

https://doi.org/10.26637/MJM0804/0137

Construction of a chaotic map-based authentication protocol for online telemedicine services

Meena Sanjay Babulal [1]*

Abstract

Upgraded network technology yields a new interface "telecare medicine information systems" in short TMIS, between patient and server. But, it can be observed that these services generally insecure as the information being transmitted over a public channel. Chaotic map plays highly important role in designing an authentication protocol, and a good candidate to ensure the efficiency. Although few of the protocols needs low computation cost, but they cannot establish an anonymous communication. Keeping these facts in mind, one needs to construct a chaotic map based authentication scheme for a TMIS. Moreover, we have done performance analysis of related schemes to show the advantage of our work.

Keywords

Chaotic-Mapping, Authentication, Finite Field, Security, Privacy.

AMS Subject Classification

81Q50, 37D99, 11G20, 11T55, 94A62.

[1] *Department of Mathematics, University of Rajasthan, Jaipur-302004, India.*

***Corresponding author**: [1] sanjaymeena.iitb@gmail.com

Article History: Received **13** September **2020**; Accepted **20** November **2020**

Contents

1. Introduction

Telemedicine is an emerging sector in medical field not only for convenience of patients but also for doctors. The pandemic Covid 19 make it necessary that initial interaction of health workers and patient should be done through online platforms. Telemedicine is not a new concept, it is traces back to the mid-20th century, when radio has been used to provide health advice on ships. For hospitals the first uses were for psychiatric services in the 1950's via a closed circuit television connection. Telemedical care has expanded over the past 30 years to include stroke, mental health and chronic deceased patients such as diabetes, asthma or heart failure.

With the increasing growth of mobile and software related applications, Telemedicine services will potentially provide essential healthcare coverage for rural and remote areas where advanced medical knowledge is unavailable. Since the Internet is really an open network with multiple possible safety holes, careful attention and precautions must be exercised to ensure medical and patient data protection.

Healthcare and treatment have long been one of the highly important issue of humans. On the lines of current development in variety of medical sensors one can measure various physiological signs of the human body using smartphones, smart sensors, which always accompany the users. Computer science possesses an important place in healthcare and treatment domain, where various research as well as projects have

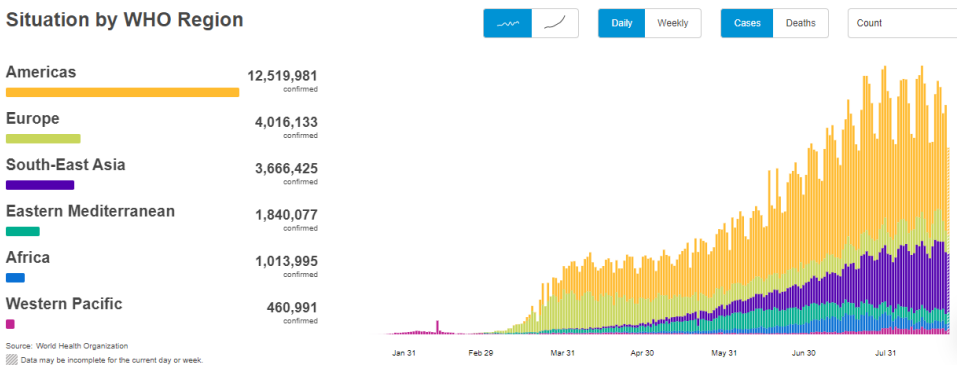

Figure 1. world wide data of covid-19 reported on August 25, 2020 by WHO

been going on and completed. Nowadays, both computer science and information technology are promoting healthcare services (see Fig. 1, 2) around the world. Employing robots and smart sensors in surgeries, machine learning and artificial intelligence techniques in medical diagnosis, pervasive computing systems for any time, anywhere and medical care, and distributed systems for processing big data of medical are just a few examples of computer based applications in healthcare.

One of the highly important system TMIS is very useful in various healthcare services remote areas such as medical monitoring, consultation, and other health conscious and necessarily convenient services, which are the current demand in various healthcare sectors. These services facilitates private health related support to the concerned patient at their home. Everyday, both engineer and researcher are developing innovative ideas to develop advanced healthcare services.

Therefore, the people can be facilitated with health-services through their smart phone, i-pads, and other electronic devices, where privacy of the users and their access to the service plays highly important role. Therefore, Wu et al. [9] deisgned an advanced authentication protocol to benefit the healthcare services. In 2012, Wei et al. [8] observes [9] is vulnerable to two-factor authentication. Therefore, a new design comes in demand under two-factor authentication. Zhu [11] shows password guessing in [8] and introduced an improved scheme, but he did not think about anonymous communication. Chen et al. [3] introduced highly demanding authentication protocol preserving anonymous communication (in TMIS services). Lin et al. [6] observes weakness in [3] as identity can be revealed using the dictionary and password guessing can be done with stolen smart card. Therefore, he invented an anonymous protocol to emove most of the existing attacks. Cao and Zhai [2] also found that [3] is not resistant against identity guessing and password with the information of smart card. These schemes [2, 6, 11] vulnerable to input verifying condition due to which these schemes cannot efficiently distinguish incorrect input. Two highly important attributes are anonymity and unlinkability, which are missing in [8, 9, 11, 31].

To improve the efficiency and security chaotic cryptosystems has been developed. In 2013, Guo et al. [13] introduced a new authentication scheme using chatic-cryptosystem, but Hao et al. [14] claims that both user's traceability and two secret keys are the main issues. Therefore, Hao et al. introduced a new scheme better than [13]. Jiang et al. [15] carefully analysed the weakness in [14] i. e. stolen smart card attack.

Li et al. [20] designed an advanced chaotic map-based authentication protocol used to healthcare services, Madhusudhan et al. [19] analysed various attacks such as password guessing, and impersonation. Jiang et al. [27] designed an improved TMIS, but it exchanges three messages to estabilish secure session key. Wu et al. [28] introduced Rfid based authentication and Radhakrishnan et al. [18] designed an advanced TMIS, but it is also vulnerable to password, identity guessing and stolen smart card attacks. Zhang et al. [24] introduced demanding advanced authentication protocol for heathcare TMIS, but it is also vulnerable to various attacks such as identity, password and replay. Madhusudhan et al. [19] designed a robust protocol used to telecare medical information system, it can be observed their scheme is suffering identity, password, impersonation, and stolen smart card attacks. Recently, Dharminder et al. [33] proposed a new construction of RSA based authentication in authorized access to healthcare services, but it uses costly modulo exponentiation.

From Table 2, one can observe security analysis of chaotic based authentication in TMIS, where notation $\surd$ stands for "yes", and $\times$ for "not". Table 1, 2 shows that existing schemes for TMIS faces various vulnerabilities. Therefore, we need a new TMIS using chaotic-system with the following features:

- Both user login and password change must be efficient.
- Linkability, identity and password guessing resistant.
- Security and efficiency.

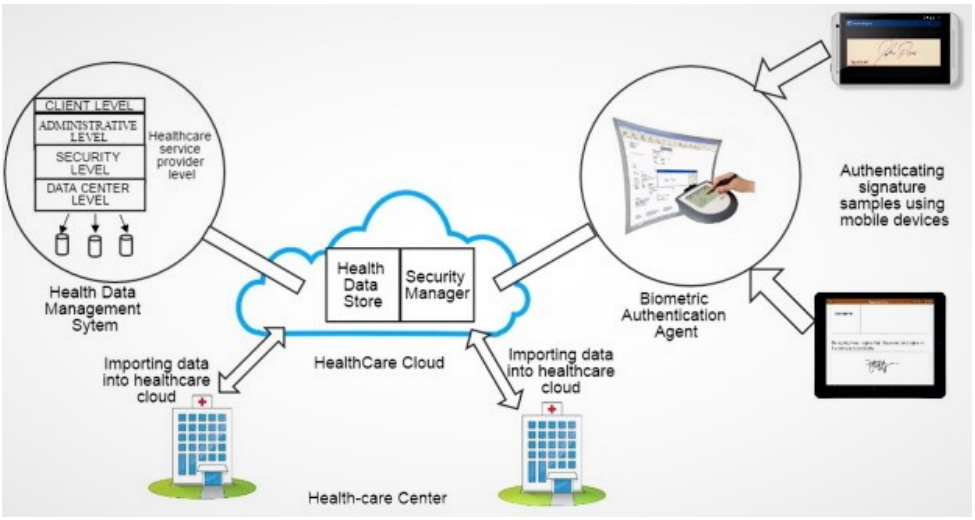

Figure 2. A typical model of health-care services with respect to authentication protocol

Security attributes\Schemes	[3]	[2]	[10]	[6]	[29]	[23]	[12]	[30]
Anonymous	√	√	√	√	√	√	√	×
Password-guessing	×	×	×	√	√	√	×	×
Stolen-card	√	√	√	√	√	√	√	√
Impersonation	×	√	√	√	√	√	×	√
Replay-attack	√	×	√	√	√	√	√	√
Linkability	×	√	√	√	√	×	×	×
Key-agreement	√	√	√	√	√	√	√	√
Session key verification	×	√	×	×	×	√	×	×
Password-change	√	√	×	×	×	×	×	√

Table 1. Security comparison of password based authentication schemes for TMIS

Therefore, a new scheme has been designed along with both security and efficiency using chaos theory based cryptosystem. This scheme essentially analysed in random Oracle as well as using BAN logic. Another important contribution of the scheme to resist session key violation introduced by Bergamo et al. [32].

2. Preliminaries

Notations and basic definitions are discussed to analyze some properties of Chaos theory and the scheme. The brief description of the used notations are given as in Table 3.

2.1 Chebyshev Chaotic Mapping

Chaotic mapping possesses an advanced structure (as shown in Figure 3) in nonlinear dynamics, and its security and pseudo randomness. We are basically trying to illustrate some of basic definition and necessary properties in brief could be found in [16].

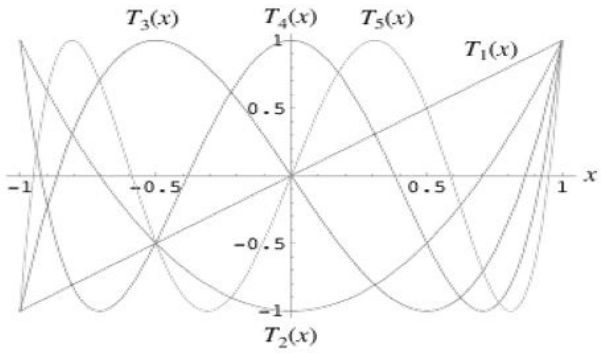

Figure 3. Chebyshev polynomials

- **Definition 1** Chebyshev proposed a polynomial essentially in variable "x" described as $T_\kappa(x) : (-\infty, +\infty) \to [-1, +1]$ of positive degree κ, whereas $T_\kappa(x) = cos(\kappa(arccos(x)))$ and the recurrence

Security attributes/Schemes	[23]	[14]	[21]	[22]	[24]	[18]	[20]	[19]
Anonymous	√	√	×	√	×	×	×	×
Linkability	×	√	√	√	√	×	√	×
Insider-attack	√	√	√	√	√	√	√	√
Password-guess	√	√	√	√	×	×	×	×
Stolen-card	√	√	√	√	√	×	√	×
Impersonation-user	√	√	√	√	√	√	×	×
Impersonation-server	√	√	√	√	√	√	×	×
Replay	√	√	√	√	×	√	√	√
Key-agreement	√	√	√	√	√	√	√	√
Key-verification	√	×	√	×	√	√	×	√

Table 2. Security comparison of chaotic map-based authentication schemes for TMIS

Table 3. Notations and Symbols

Notation	Description
U_i	User-i
S_j	Server-j
$\mathscr{A}$	Adversary
Sc_i	Smart Card
ID_i	Identity of U_i
$TMIS$	Telecare medicine information system
PW_i	Password of U_i
s	Secret value of S_j
$h(\cdot)$	A collision resistant hashing
$h_b(\cdot)$	A collision resistant biometric-hashing
$\oplus$	Bitwise XOR
$\|\|$	String concatenation

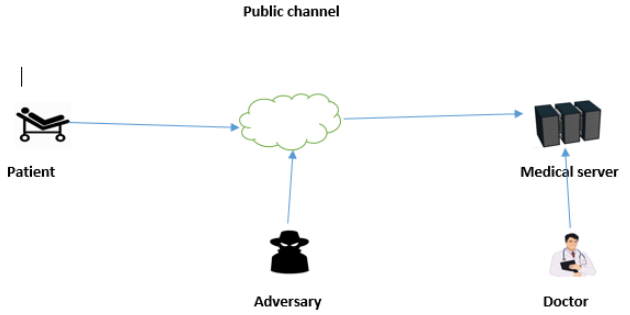

Figure 4. Communication model in TMIS

$T_\kappa(x)$ is defined as $T_\kappa(x) = (2xT_{\kappa-1}(x) - T_{\kappa-2}(x))$, whereas $x \in (-\infty, +\infty)$ and $T_0(x) = 1$, $T_1(x) = x$.

- **Definition 2** Discrete Logarithm Problem (DLP) is defined for known y and x, it is computationally infeasible to find u such that $T_u(x) = y$.

- **Definition 3** Computational Diffie-Hellman Problem (CDHP) is to find out $T_{uv}(x)$ if one essentially knows x, $T_u(x)$ and $T_v(x)$.

2.2 Threat model

In this subsection, we are assuming a threat model as in Figure(1) and notations in Table 3 under the scheme [7], where $\mathscr{A}$ possesses some computational resources and smart card security in both password and chaotic based authentication schemes.

- The user essentially chooses an arbitrary pseudo-random password from the dictionary. Server generates its own concerned private key and inserts essential values in the smart card.

- $\mathscr{A}$, U_i and S_j interact via executing oracle queries that allow $\mathscr{A}$ to simulates an attack on the authentication protocol.

- Communication channel is controlled and managed by the $\mathscr{A}$, where interception, modification, sending again the messages and divert the message are possible.

- The $\mathscr{A}$ may also steal the information stored in smart card.

3. Proposed authentication protocol under chaotic mapping

We have proposed an advanced chaotic mapping based authentication protocol, that has been divided into four phases, (1) registration, (2) login, (3) authentication and (4) password update respectively.

3.1 Registration-Phase

U_i executes the registration process (see Fig 5) along with S_j via a private channel as described in the following lines.

- U_i selects ID_i, PW_i, and imprints his own biometric $H_i = h_b(biometric)$, then he does the computation $A_i = h(ID_i||PW_i||H_i)$ and transmits $\{ID_i, A_i\}$ to corresponding S_j.

- After getting the information $\{ID_i, A_i\}$, S_j stores ID_i of U_i and it computes $x = h(ID_i||s)$, where "s" is the secret key of server S_j. Now, S_j chooses arbitrary $n_i \in Z_p^*$, then

it computes $T_x(ID_i||n_i)$ that corresponds to U_i. Furthers, it computes the value $B_i = T_x(ID_i||n_i) \oplus A_i$.

- S_j delivers a hidden information $\{h(.),\ B_i,\ n_i\}$ stored in the smart-card that is given to U_i via a private channel.
- Finally, U_i does the computations $T_x(ID_i||n_i) = B_i \oplus A_i$, $D_i = h(T_x(ID_i||n_i)||PW_i||ID_i||H_i)$, $N_i = n_i \oplus A_i$ and store D_i with the corresponding values $\{h(.),\ B_i,\ D_i,\ N_i\}$.

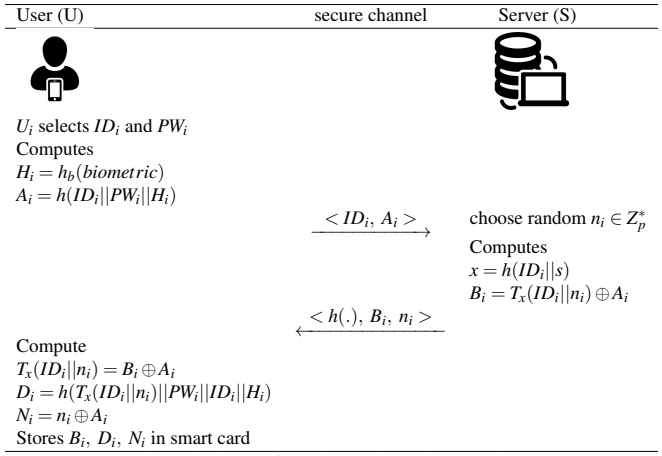

Figure 5. A description of registration phase via secure channel

3.2 Login Phase

A legal U_i tries to get login to corresponding S_j in the following steps:

- U_i inputs the card, ID_i and PW_i, then he computes $H_i = h_b(biometric)$ and $A_i' = h(ID_i||PW_i||H_i)$.
- Using A_i' smart card executes the step $T_x(ID_i||n_i)' = A_i' \oplus B_i$ and computes $D_i' = h(T_x(ID_i||n_i)'||PW_i||ID_i||H_i)$ and proceeds for the legal verification $D_i' =? D_i$.
- The card takes input an arbitrary $y \in Z_p^*$ and furthers proceeds to compute $Sk_i = T_yT_x(ID_i||n_i)$, $C_i = T_y(ID_i||n_i)$, $NID_i = ID_i \oplus Sk_i$ and $F_i = h(T_y(ID_i||n_i)||T_x(ID_i||n_i)||Sk_i)||T_1)$, and then U_i transmits $\{C_i,\ F_i,\ NID_i,\ T_1\}$ to S_j.

3.3 Authentication Phase

S_j receives $\{C_i,\ F_i,\ NID_i,\ T_1\}$ from corresponding U_i and executes the process of authentication (see Fig 6):

- S_j verifies the time stamp T_1, and furthers obtains $T_y(ID_i||n_i) = C_i'$, then it does the computation $T_xT_y(ID_i||n_i) = Sk_i'$, $F_i' = h(C_i'||T_x(ID_i||n_i)||Sk_i'||T_1)$, then it verifies the values $F_i' = F_i$ are equal or not.
- S_j performs the computation $Z_i = h(Sk_i||ID_i||T_2)$ and transmits the information $\{Z_i,\ T_2\}$ to corresponding U_i.
- After receiving the information $\{Z_i,\ T_2\}$ from S_j, then U_i confirms the time stamp T_2 is valid or not, then he computes $Z_i' = h(Sk_i'||ID_i||T_2)$, and proceeds the verification $Z_i' = Z_i$, and establishes a session key $Sk = T_xT_y(ID_i||n_i)$.

3.4 Password update phase

U_i can have access to update the password executing the following steps:

- U_i inputs the card Sc_i, ID_i and PW_i. Furthers, he imprints biometric, then computes $H_i = h_b(biometric)$ and $A_i' = h(ID_i||PW_i||H_i)$. Using A_i' the Sc_i obtains $T_x(ID_i||n_i)' = A_i' \oplus B_i$ and $D_i' = h(T_x(ID_i||n_i)'||PW_i||ID_i)$, and proceeds for the verification $D_i' = D_i$.
- U_i inputs Pwd_i^{new} then Sc_i and proceeds the computation $A_i^{new} = h(ID_i||PW_i^{new}||H_i)$, $D_{new} = h(T_x(ID_i||n_i)||PW_{new}||ID_i||H_i), B_i^{new} = A_i^{new} \oplus T_x(ID_i||n_i)$ and updates the values B_i, D_i with B_i^{new}, D_i^{new}.

4. Security Analysis

4.1 Security proof in Random oracle

Initially, we need to describe a model $\mathscr{P}$ to validate the security of the proposed scheme and then we will implement the proposed protocol under random oracle (RO).

Security-Model Let $C_i \in (U_i,\ S_j)$ be an i^{th} instance, where $\mathscr{A}$ is an adversary who controls communication between U_i and S_j.

Extract: This phase actually permits $\mathscr{A}$ to retrieve corresponding private key of U_i.

Send(M, C_i)**:** This permits $\mathscr{A}$ to send arbitrary message M, then Oracle sends the final output to $\mathscr{A}$.

Hash(m): $\mathscr{A}$ sends arbitrary m to the hashing $H(.)$, it chooses arbitrary $s \in Z_p^*$ and stores (m,s) and returns the arbitrary number.

Reveal(C_i)**:** This permits $\mathscr{A}$ to get the knowledge about CK_{ij} (session key), when an Oracle gets a reveal query.

Corrupt(C_i)**:** This allows $\mathscr{A}$ to disturb and to make a corruption to the party C_i and it obtains key of the corrupted party C_i.

Test(C_i)**:** This permits Oracle to receive a message from $\mathscr{A}$, then Oracle guesses a $c \in \{0,1\}$. If c = 0, then it sends an arbitrary random number, and If c = 1, then oracle return a session key CK_{ij}.

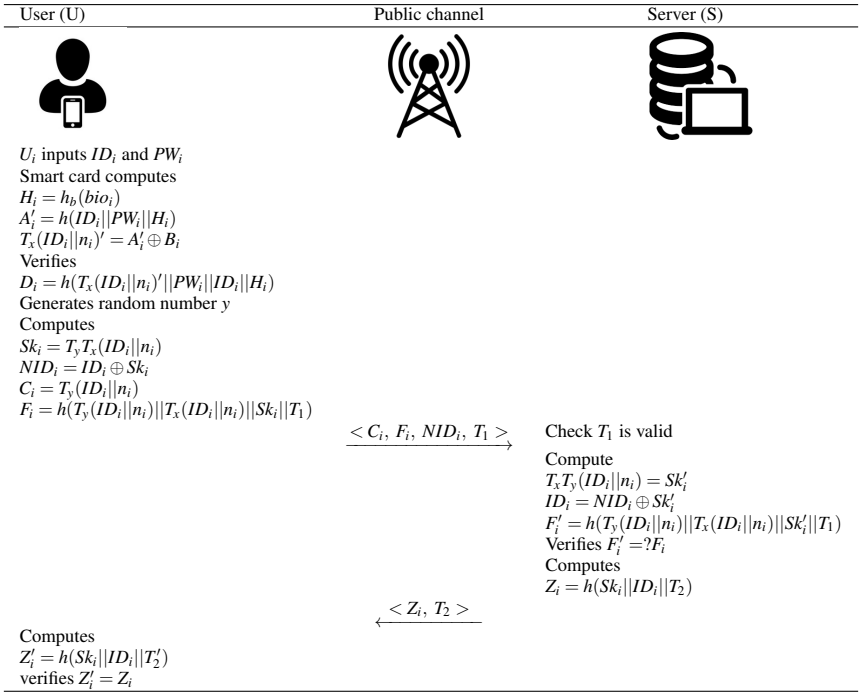

Figure 6. A description of of login and authentication phases

Let $Succ(\mathscr{A})$ successfully guess the value of a bit c, which is chosen from the corrupt query phase. The advantage held by the $\mathscr{A}$ against the authentication protocol is defined as:

$$Adv_{\mathscr{A},P}(k) = |2.Pr[Succ(\mathscr{A})] - 1|$$

Security analysis for the proposed scheme achieves mutual authentication in RO.

Chaotic based assumption: For random oracle construction on chaotic map, basic primitive as follows: From generation algorithm $Gen(1^n) = p$, where p is prime of length n and $x \in Z_p^*$ is secret key of S_j.
$\forall$ probabilistic polynomial time adversary $\mathscr{A}$, $\exists$ a negligible function $neg(n)$ such that:

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

$$: \mathscr{A}(1^n, p, T_x(r)) \rightarrow x] = neg(n)$$

Collision resistance attack(CRA) algorithm: If $\mathscr{A}$ finds a collision for a one way hash function $h(.)$, we have

$$Ad_{\mathscr{A}} = Pr[(x,x') \overset{R}{\leftarrow} Ad : x \neq x' and h(x) = h(x')]$$

Theorem 4.1. *Let H be a random Oracle and $\mathscr{A}$ be an adversary, then we will model an algorithm B who solve CAA problem using subroutine $\mathscr{A}$.*

Proof *Initially, B receives an instance C_i, F_i, H_i and then B tries to solve the CAA instance via computing X_i* and $r*$ and checking the conditions $h(r^*||ID_i||PW_i) = ?D_i$ or $F_i = ?h(T_y(ID_i||N_i)||Sk_u||T_1)$. Finally, the information H, ω, p, T, $Gen(.)$ is made public for B, who can approach to $\mathscr{A}$.*

H hash query: *When $\mathscr{A}$ submits a query which corresponds to ID_i, then B carefully first verifies ID_i in H_{ij} list. If present in the list named H_{ij}, then B returns exactly the value h_{i1}, otherwise it computes the value $h_a = H_1(ID_i)$ and puts in the list along with $(ID_i,\ h_a)$, and sends back h_a to $\mathscr{A}$.*

Extract: *$\mathscr{A}$ submits an advanced query on ID_i, then B receives the corresponding query and proceeds for the verification $H_1(ID_i) \in \{C_i, F_i, T_i\}$. If verification does not hold, then B terminates the process. After following this procedure, B goes for the verification $ID_i \in H_{ij}$, if present, then it give response, else calculates $X_i = T_y(ID_i||N_i)$ and $D_i = h(T_x(ID_i||N_i)||PW_i||ID_i||\theta_i)$ returns to $\mathscr{A}$.*

Send-queries: *Send phase is described as below U_i login and sends a message $< (C_i, F_i, T_1) >$ to S_j, and S_j responds (H_i, T_2). This phase is described with the help of a game played between U_i and S_j respectively.*

1. *$\mathscr{A}$ sends a query, then B returns a login message to $\mathscr{A}$.*
2. *To get login in to S_j, $\mathscr{A}$ submits polynomial times send queries, then B does a computation corresponding to i^{th} query as $X_i = T_y(ID_i||N_i)$ and $V_i = h(T_x(ID_i||N_i)||Pw_i||N_i)$ responds to $\mathscr{A}$.*
3. *$\mathscr{A}$ submits $(V_i,\ U_i)$, then B verifies first whether $H(ID_i) \in H_{ij}$ or not. If it is present, then B returns a*

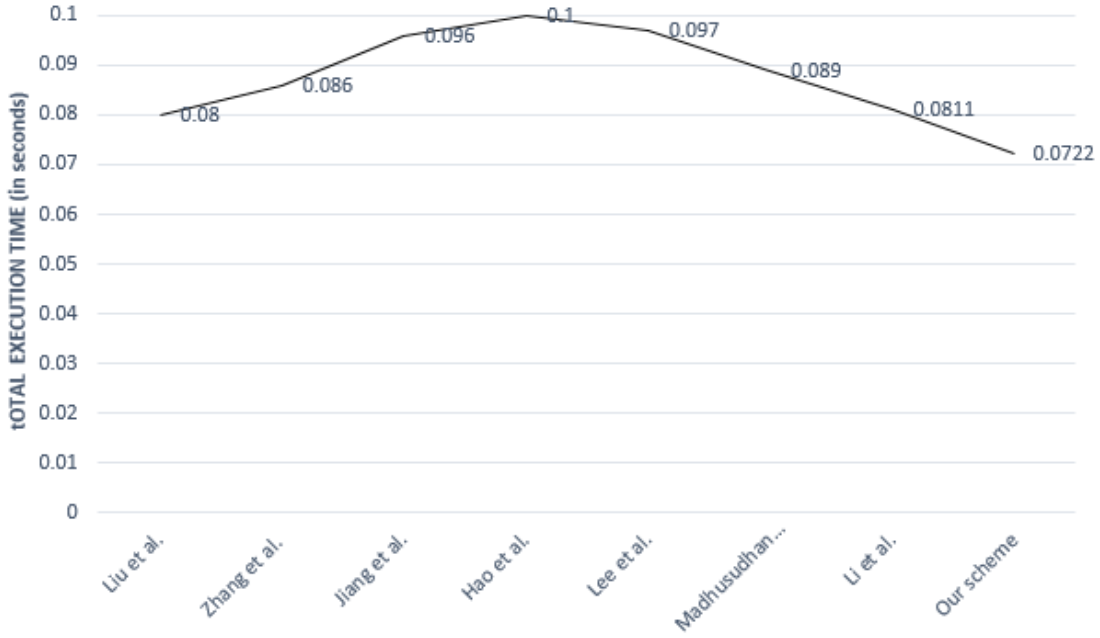

Figure 7. Computation cost comparison

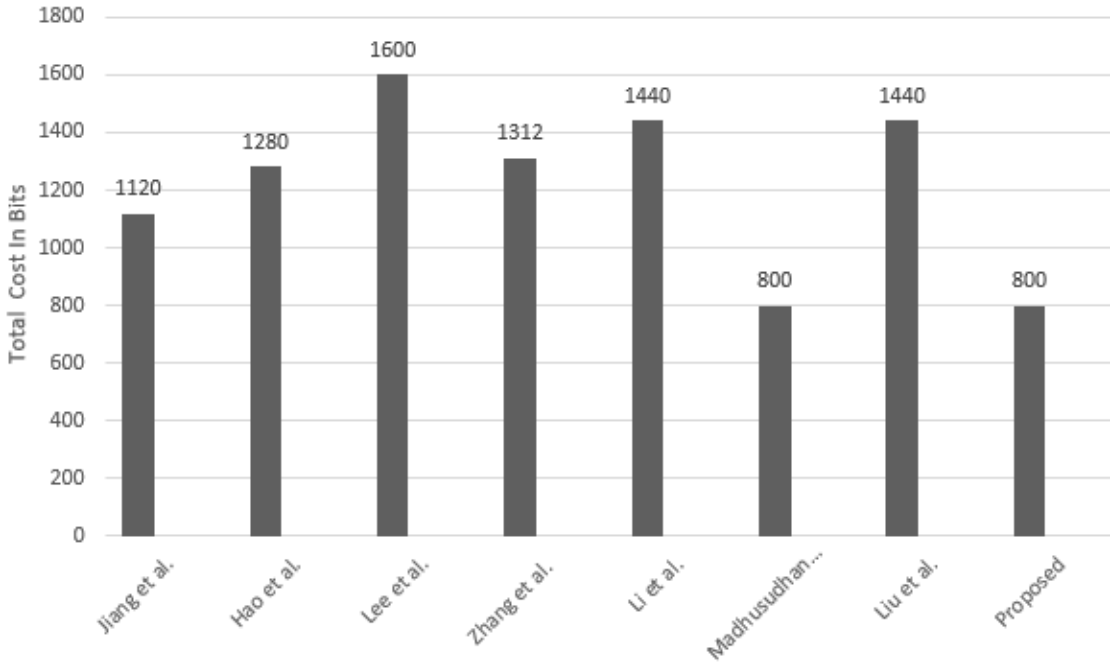

Figure 8. Communication cost comparison

failure, otherwise it terminates the query E_{e_1}. *Furthers, B computes* $M_1 = T_y(ID_i||N_i)$, *and* $Sk_u = T_z T_y(ID_i||N_i)$ *for arbitrary z, y and* $F_i = h(T_y(ID_i||N_i)||Sk_u||T_1)$ *and returns the output to* $\mathscr{A}$.

4. *$\mathscr{A}$ submits $((C_i,F_i),LS_j)$, then B computes $X_i = h(Id_i||r)$ and $D_i = h(r||ID_i||PW_i)$, where r is an arbitrary number, and verifies the equation $D_i = ?h(r||Id_i||Pw_i)$, if holds, then B does the computation $Sk_s = T_yT_z(ID_i||N_i)$, $H_i = h(Sk_s||T_2)$ responds (H_i,T_2) to $\mathscr{A}$.*

5. *$\mathscr{A}$ submits $((H_i,T_2),U_i)$, then B finds out H_i with the help of computation done above and proceeds the checking $H_i* = ?h(Sk_s||ID_i||T_2)$ and finally authenticates $\mathscr{A}$ respectively.*

Analysis If $\mathscr{A}$ is able to forge C_1 without knowing any partial information about the private key, then it sends a duplicate F_i*. If $C_1 = h(X) \in H_{ij}$, then failure happens in the process E_{e_2}. Otherwise, B is able to solve the CAA problem. As $H(ID_i) \notin H_{ij}$, $Z = h(Y) \notin (x_{i1},x_{i2}\dots)$, and δ be chance of success of B, and ε be the chance of breaching the scheme respectively. Then, each of the queries hashing, extracts and sends are legal when event E_e , E_{e_1}, E_{e_2} exist. So, B takes the help of $\mathscr{A}$ to break CAA problem, if none of E_e , E_{e_1}, E_{e_2} happened. Thus,

$$Pr[\neg E_e \wedge \neg E_{e_1} \wedge \neg E_{e_2}] = \left(\frac{q_E}{q_H}\right)^{q_E+q_s}\left(\frac{q_H-q_E}{q_H}\right)$$

Therefore, B is successful with advantage

$$\delta \geq \left(\varepsilon - \frac{1}{2^k}\right)\left(\frac{q_E}{q_H}\right)^{q_E+q_s}\left(\frac{q_H-q_E}{q_H}\right)$$

So, the algorithm B has gain the advantage as above, therefore if $\mathscr{A}$ gets success in breaking the protocol, then B can use subroutine $\mathscr{A}$ to break the proposed scheme.

5. Performance Analysis

The performance analysis describes efficiency of the proposed protocol as compared to the related protocols in Table 4, where $t_h \approx 0.0005s$, $t_{sym} \approx 0.0087s$, $t_c \approx 0.02102s$ and $t_m \approx 0.06307s$ denote the time of computation hashing, symmetric-encryption, chaotic-map operation, multiplication in Z_p^* respectively.

Schemes	User-computation	Server-computation	Messages
Liu et al.'s [21]	$4t_h+2t_c$	$5t_h+2t_c$	3
Jiang et al.'s [15]	$2t_h+t_{sym}+t_c$	$2t_h+2t_{sym}+3t_c$	2
Hao et al.'s [14]	$2t_c+3t_h+2t_{sym}$	$2t_c+3t_{sym}+2t_h$	2
Lee's [23]	$2t_c+7t_h$	$2t_c+8t_h$	2
Zhang et al.'s [24]	$6t_h+2t_c$	$4t_h+1t_c+2t_{sym}$	3
Madhusudhan et al's [19]	$7t_h+2t_c$	$3t_h+2t_c$	2
Li et al.'s [1]	$7t_h+2t_c$	$7t_h+2t_c$	2
Proposed	$3t_c+2t_h$	$2t_c+2t_h$	2

Table 4. An analysis of performance with recent chaotic map-based authentication protocols

This section presents a performance analysis of authentication schemes [1, 14, 15, 19, 21, 23, 24]. All the schemes related to telecare medicine services highly depend on operations which requires low computation and limited storage. Both efficiency and performance has been compared to the related protocols in Table 4, whereas the cost of each operation is computed via running the experiment on intel $Pentium-4$ processor with 1024 MB ram as in [5, 34] along with computation cost illustrated in Figure 7.

Moreover, Liu et al.'s scheme [21] takes $4t_h++2t_c$ for user, $5t_h+2t_c$ for server, Jiang et al.'s scheme [15] takes $2t_h+t_{sym}+t_c$ for user, $2t_h+2t_{sym}+3t_c$ for server, Hao et al.'s scheme [14] takes $2t_c+3t_h+2t_{sym}$ for user, $2t_c+3t_{sym}+2t_h$ for server, Lee et al.'s scheme [23] takes $2t_c+7t_h$ for user, $2t_c+8t_h$ for server, Zhang et al.'s scheme [24] takes $6t_h+2t_c$ for user, $4t_h+1t_c+2t_{sym}$ for server, Madhusudhan et al's scheme [19] takes $7t_h+2t_c$ for user, $3t_h+2t_c$ for server, Li et al.'s scheme [1] takes $7t_h+2t_c$ for user, $7t_h+2t_c$ for server, where the presented protocol executes $3t_c+2t_h$ for user, $2t_c+2t_h$ for server respectively.

In this paper, we adopt the communication cost of hash function, chaotic map and time stamp are given the 160-bit output, and symmetric encryption is 256 bits, where total communication overhead is given in Figure 8. The computation comparison of proposed schemes is shown in Figure 8.

6. Conclusion

This article describes the security of recently presented chaotic map based authentication in the random Oracle. The proposed protocol successfully removes the existing vulnerabilities and observes that how a poor verification invites various attacks. Furthermore, it can be observed that the presented design ensures session key verification after just two messages exchange.

References

[1] Li, Xiong and Wu, Fan and Khan, Muhammad Khurram and Xu, Lili and Shen, Jian and Jo, Minho: A secure chaotic map-based remote authentication scheme for telecare medicine information systems Future Generation Computer Systems **84**0 (2018) 149-159.

[2] Cao, T., Zhai, J.: Improved dynamic id-based authentication scheme for telecare medical information systems. Journal of Medical Systems **37**(2) (2013) 1–7.

[3] Chen, H.M., Lo, J.W., Yeh, C.K.: An efficient and secure dynamic id-based authentication scheme for telecare medical information systems. Journal of Medical Systems **36**(6) (2012) 3907–3915.

[4] Avoine, Gildas Adversarial Model for Radio Frequency Identification IACR Cryptology ePrint Archive Citeseer (2005) 1–49.

[5] Kocarev, Ljupco and Lian, Shiguo Chaos-based cryptography: theory, algorithms and applications Springer Science and Business Media Springer (2011) 330–354.

[6] Lin, H.Y.: On the security of a dynamic id-based authen-

tication scheme for telecare medical information systems. Journal of Medical Systems **37**(2) (2013) 1–5

[7] Dolev, Danny and Yao, Andrew On the security of public key protocols IEEE Transactions on information theory IEEE (1983) 198–208.

[8] Wei, J., Hu, X., Liu, W.: An improved authentication scheme for telecare medicine information systems. Journal of Medical Systems **36**(6) (2012) 3597–3604

[9] Wu, Z.Y., Lee, Y.C., Lai, F., Lee, H.C., Chung, Y.: A secure authentication scheme for telecare medicine information systems. Journal of Medical Systems **36**(3) (2012) 1529–1535

[10] Xie, Q., Zhang, J., Dong, N.: Robust anonymous authentication scheme for telecare medical information systems. Journal of Medical Systems **37**(2) (2013) 1–8

[11] Zhu, Z.: An efficient authentication scheme for telecare medicine information systems. Journal of Medical Systems **36**(6) (2012) 3833–3838

[12] Jiang, Q., Ma, J., Ma, Z., Li, G.: A privacy enhanced authentication scheme for telecare medical information systems. Journal of Medical Systems, **37**(1) (2013) 1–8

[13] Guo, C., Chang, C.C.: Chaotic maps-based password-authenticated key agreement using smart cards. Communications in Nonlinear Science and Numerical Simulation **18**(6) (2013) 1433–1440.

[14] Hao, X., Wang, J., Yang, Q., Yan, X., Li, P.: A chaotic map-based authentication scheme for telecare medicine information systems. Journal of Medical Systems **37**(2) (2013) 1–7.

[15] Jiang, Q., Ma, J., Lu, X., Tian, Y.: Robust chaotic map-based authentication and key agreement scheme with strong anonymity for telecare medicine information systems. Journal of Medical Systems **38**(2) (2014) 1–8.

[16] Kohda, T., Tsuneda, A., Lawrance, A.J.: Correlational properties of chebyshev chaotic sequences. Journal of time series analysis **21**(2) (2000) 181–191.

[17] Kohda, T., Tsuneda, A.: Pseudonoise sequences by chaotic nonlinear maps and their correlation properties. IEICE Transactions on Communications **76**(8) (1993) 855–862.

[18] Radhakrishnan, Niranchana and Karuppiah, Marimuthu An efficient and secure remote user mutual authentication scheme using smart cards for Telecare medical information systems Informatics in Medicine Unlocked year Elsevier (2018) 1–38.

[19] Madhusudhan, R and Nayak, Chaitanya S.: A robust authentication scheme for telecare medical information systems. Multimedia Tools and Applications. Springer (2018) 1–19.

[20] Li, Chun-Ta and Lee, Cheng-Chi and Weng, Chi-Yao and Chen, Song-Jhih A secure dynamic identity and chaotic maps based user authentication and key agreement scheme for e-healthcare systems. Journal of medical systems. Springer (2016) 11–233.

[21] Liu, Yu and Xue, Kaiping An improved secure and efficient password and chaos-based two-party key agreement protocol Nonlinear Dynamics Springer (2016) 549–557.

[22] Li, Chun-Ta and Lee, Cheng-Chi and Weng, Chi-Yao A secure chaotic maps and smart cards based password authentication and key agreement scheme with user anonymity for telecare medicine information systems Journal of Medical Systems Springer (2014) 9–86.

[23] Lee, T.F.: An efficient chaotic maps-based authentication and key agreement scheme using smartcards for telecare medicine information systems. Journal of medical systems **37**(6), 1–9 (2013)

[24] Zhang, Liping and Zhu, Shaohui and Tang, Shanyu Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme IEEE journal of biomedical and health informatics IEEE (2017) 465–475

[25] Amin, Ruhul and Biswas, GP : An improved rsa based user authentication and session key agreement protocol usable in tmis. Journal of Medical Systems. Springer (2015) 8–87.

[26] Burrows, M., Abadi, M., Needham, R.M.: A logic of authentication. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences **426**(1871) (1989) 233–271.

[27] Jiang, Qi and Chen, Zhiren and Li, Bingyan and Shen, Jian and Yang, Li and Ma, Jianfeng Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems. Journal of Ambient Intelligence and Humanized Computing Springer (2018) 1061–1073.

[28] Wu, Fan and Xu, Lili and Kumari, Saru and Li, Xiong and Das, Ashok Kumar and Shen, Jian A lightweight and anonymous RFID tag authentication protocol with cloud assistance for e-healthcare applications Journal of Ambient Intelligence and Humanized Computing Springer (2018) 919–930.

[29] Xu, X., Zhu, P., Wen, Q., Jin, Z., Zhang, H., He, L.: A secure and efficient authentication and key agreement scheme based on ecc for telecare medicine information systems. Journal of Medical Systems **38**(1) (2014) 1–7

[30] Wu, F., Xu, L.: Security analysis and improvement of a privacy authentication scheme for telecare medical information systems. Journal of Medical Systems **37**(4), 1–9 (2013).

[31] Lee, T.F., Chang, I.P., Lin, T.H., Wang, C.C. A Secure and Efficient Password-Based User Authentication Scheme Using Smart Cards for the Integrated EPR Information System Journal of Medical Systems, **37**(3) (2013) 1–7.

[32] Bergamo, Pina and D'Arco, Paolo and De Santis, Alfredo and Kocarev, Ljupco Security of public-key cryptosystems based on Chebyshev polynomials IEEE Transactions on Circuits and Systems, **52**(7) (2005) 1382-1393.

[33] Dharminder, Dharminder and Mishra, Dheerendra and Li, Xiong Construction of RSA-Based Authentication Scheme in Authorized Access to Healthcare Services

Journal of medical systems, **44**(1) (2020) 1–6.

[34] Dharminder, Dharminder and Gupta, Pratik Security analysis and application of Chebyshev Chaotic map in the authentication protocols International Journal of Computers and Applications, **0**(0) (2019) 1–9.

⋆⋆⋆⋆⋆⋆⋆⋆⋆

ISSN(P):2319 – 3786

Malaya Journal of Matematik

ISSN(O):2321 – 5666

⋆⋆⋆⋆⋆⋆⋆⋆⋆