Soft Computing (2021) 25:8905–8920
https://doi.org/10.1007/s00500-021-05781-7

METHODOLOGIES AND APPLICATION

An effective mobile-healthcare emerging emergency medical system using conformable chaotic maps

Chandrashekhar Meshram[1] · Rabha W. Ibrahim[2] · Mohammad S. Obaidat[3,4,5] · Balqies Sadoun[6,7] · Sarita Gajbhiye Meshram[8] · Jitendra V. Tembhurne[9]

Accepted: 30 March 2021 / Published online: 26 May 2021

Abstract
The developments in telecommunication and online facility resolutions help to connect the digital divide among urban and rural healthcare services administrations, empowering arrangement of appropriate medicinal finding and treatment discussions. Mobile-healthcare (*m*-Healthcare) systems can be used for quality improvement of healthcare and monitoring individuals with chronic diseases like heart disease and diabetes under medical affair. Wireless body area networks are installed in the human body, which transmit the information via Bluetooth or other means to the smartphone. In this study, we introduce a new efficient mobile-healthcare emerging emergency medical system using conformable chaotic maps under cloud computing environment.

Keywords Mobile-healthcare emerging emergency · Smart health homes · Anonymity · Fractional calculus · Conformable chaotic maps · Mutual authentication · Opportunistic computing

1 Introduction

In cloud computing, Internet-based resources such as hardware/software are available for access and sharing. Nowadays, this is used to decrease paper work and manpower in every sector. Cloud computing's general objective is to handle complexity in an efficient manner where simplification is adopted to accelerate the utilization of capacities. Moreover, smartphones and tablet computers are becoming progressively important components of human life. They are most efficient and expedient communication instruments, which do not bound by moment

✉ Chandrashekhar Meshram
cs_meshram@rediffmail.com

Rabha W. Ibrahim
rabhaibrahim@yahoo.com

Mohammad S. Obaidat
msobaidat@gmail.com; m.s.obaidat@ieee.org

Balqies Sadoun
sadounbalqies@gmail.com

Sarita Gajbhiye Meshram
gajbhiyesarita@gmail.com

Jitendra V. Tembhurne
jtembhurne@iiitn.ac.in

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

2 IEEE: 94086547, Kuala Lumpur 59200, Malaysia

3 College of Computing and Informatics, University of Sharjah, Sharjah, UAE

4 King Abdullah II School of Information Technology, The University of Jordan, Amman, Jordan

5 University of Science and Technology Bejing, Beijing, China

6 College of Engineering, University of Sharjah, Sharjah, UAE

7 College of Engineering, Al-Balqa' Applied University, Al-Salt, Jordan

8 Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City, Vietnam

9 Department of Computer Science and Engineering, Indian Institute of Information Technology, Nagpur 440006, India

and location. Eventually, mobile users gained strong knowledge from multiple mobile application services such as Google Play Store and iPhone Apps, running on the computers as well as remote servers via wireless networks. Mobile Computing is a fast advancement that have become a strong trend in IT technology growth. Hence, mobile-healthcare community has been mainly discussing mobile communication applicability and other state-of-the-art techniques, i.e., multimedia technology, which is incorporated into the mobile systems.

Broadly, deployed electronic healthcare (*e*-Healthcare) systems have enhanced people's day-by-day life. *E-Healthcare* systems compared to conventional paper-based systems provide a higher efficiency, better precision, and more extensive accessibility and flexibility. Moreover, mobile-healthcare (*m*-Healthcare) systems use compact gadgets to encourage the use of *e*-Healthcare systems, which empowers patients' to efficiently and effectively save individual health information and acquire better medicinal services. Mostly, in *m*-Healthcare systems, patients utilize implantable medical devices (IMDs), sensors and smartphones to save personal health information's (PHI) (denoted by, ρ_{hi}), at that point, send medical information to the assigned healthcare foundation in order to acquire physician's diagnosis through remote interfaces.

Recently, medical experts have increasingly started to utilize smartphone (SP) as stages for conveyance of health mediations. This review concentrated on a broad spectrum of health scenarios and arose from both health sciences and computer science branches such as Human Computer Interaction (HCI) and universal calculating. Individual Digital Supporters (IDSs) certified physicians to successfully download medicinal archives, medical pictures, laboratory outcomes, and medication information in the 90 s. Patients could know about their disease control, diagnostic, and observing with SP that go with them all over the place. The worldwide telemedicine market is expected to grow up to 27.3 billion dollars approximately. There are over 70% general practitioner and 77% patients who need to get connected with *m*-Healthcare systems by utilizing their own SP's (www.research2guidance.com). Despite the reality that the Health Insurance Portability and Accountability Act (HIPAA) has been developed to regulate the *PHI*-related activities for a significant period of time, the security concern is still apparently the real boundary that impedes the deployment of *m*-Healthcare systems in view of incorporated foundations (physician's facilities or medicinal centers) (http://www.ebri.org/surveys/hcs/).

Recent developments in Electronic Health Record (EHR) technology have considerably improved the quantity of clinical information electronic accessibility (Elliot and Purdam 2008). This information, compared to medical and logical archives as well as digitalized patient health records, is important assets for clinical and translational research. The examination of the healthcare understanding captured in clinical databases may prompt enhanced progression in patient assessment, better-quality treatment, prevention of unfavorable medications responses, and in guaranteeing that an individual in danger gets suitable help services in a timely manner (Malin and Sweeney 2004). Normal *m*-Health administrations replicas use the Internet and Web-based administrations to give a legitimate communication among the authorities and patients.' A physician or a patient without much of a stretch can access a similar medical record whenever and wherever through her/his PC, tablet, or SP. The patient can interact with the physicians in the event of an emergency, or even approach medical records or arrangements regardless of time and place. A *m*-Healthcare can work when a utilization of ubiquitous computing is presented in a SP. The SP utilizes sensor nodes installed on the body to give remote healthcare assistance to the individuals (Toninelli et al. 2009; Ren et al. 2010; Li et al. 2013).

The movable communication and *m*-Healthcare construction composed a capable mean to seniors with similar side effects to share info and encounters. This gives sustenance and mutual encouragement, and empower in sending info of health situation to an associated healthcare centers through 4G communication network (Lu et al. 2011,2010a). By using *m*-Healthcare, patients equipped with SP and a wireless body sensor network (BSN) designed by sensor nodes of the body can walk absolutely external and get the needed healthcare data. Further, these data are examined and observed by physicians at whatever point and wherever without being restricted to home or physician's facility surroundings. Figure 1 indicates how inescapable health observing functions in a *m*-Healthcare system. In the first place, the BSN picks the separate mobile patient's PHI together with the rate of pulse, body temperature, blood pressure, and other vitals parameters (Lu et al. 2013). At that point, the SP totals the ρ_{hi} information through Bluetooth and delivers the info to the remote healthcare center through 4G communication networks. The physicians can persistently observe the patient's health situation in the view of the received ρ_{hi} information at the healthcare center. In the situation that the physicians at the center point out an emergency, then the staff can rapidly reply to the patient's life-threatening circumstance and keep safe life by sending off medical staffs and an ambulance to the emergency location in a speedy manner as per the received ρ_{hi} information.

The *m*-Healthcare scheme's objectives are to give fantastic ubiquitous healthcare, but the security of the system itself, is under risks. For example, in classic routine, a patient's ρ_{hi} is informed by the healthcare center once at regular intervals for ordinary remote observation (Yuce

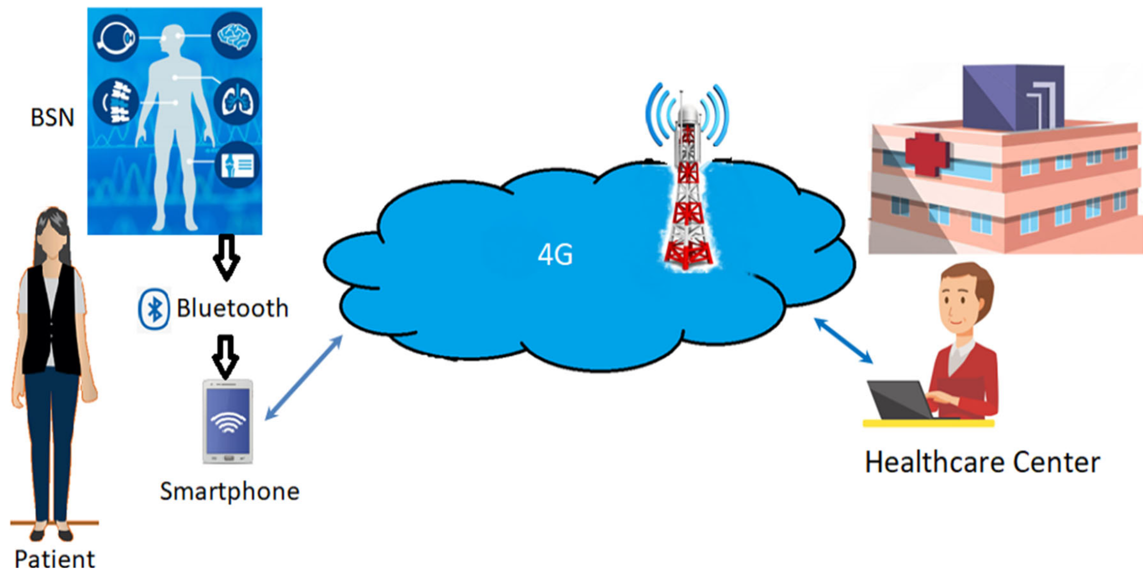

Fig. 1 Universal taxation of health in *m*-Healthcare scheme

et al. 2007; Klasnja and Pratt 2012). Nonetheless, when a patient has a scene of heart attack or is in a stroke situation, the emergency team will fix the patient's BSN in an alternate routine and make it amazingly occupied with ρ_{hi} information created at a substantially higher recurrence. At that point, the patient's ρ_{hi} information will be relayed to the healthcare center. In any case, when the emergency situation comes, the patient's SP might not have sufficient computing energy to help such high-force healthcare observing in light of the fact that it is running different applications.

Opportunistic computing has received a great interest in recent days because of the characteristic development from mobile ad hoc networks, namely MANETs (Dhurandher et al. 2018; Conti et al. 2010; Conti and Kumar 2010; Roy et al. 2020; Zhou et al. 2013; Silva Bruno and Rodrigues Joel 2015; Rault et al. 2017). In opportunistic computing, an opportunistic message among devices is sent so that the various sides can share with each other their respective assets, administrations, and substance. Thus, the scattered computing assignments under opportunistic domain can be executed by utilizing every accessible asset. The significant test of opportunistic computing is to adequately misuse opportunistic contacts to make data available and accessible, and to give community oriented processing administrations to applications and patients (Conti and Kumar 2010). With respect to ubiquitous computing, assets may include heterogeneous components of machinery, programming types, mixed media substance, sensors, and sensory information. Although not all assets can be accessed on a single gadget, any gadget can jointly access them through the development of effective middleware systems under opportunistic computing (Roy et al. 2020). There are fascinating cases of opportunistic computing applications that are now under innovative work (Lu et al. 2010a, 2013; Conti and Kumar 2010). They combine participating uncovering, global healthcare, rational moving systems, and backup administration. Lu et al. (2013) devised a SPOC framework intended for *m*-Healthcare emergency. An adaptable totaling is used to income upkeep of the uncertain dependability matter within ρ_{hi} treatment in SPOC. Other than that, Lu et al. similarly familiarized patient-centric confidentiality security Ingres control system used as a measure of the SPOC scheme, which is dependent on an attribute-based ingress control section. Another PPSPC method (Du and Atallah 2001; Vaidya and Clifton 2002; Amirbekyan and Estivill-Castro 2007; Masdari and Ahmadzadeh 2017) tried to adjust between the risk of ρ_{hi} security divulgence and the requirement of planning and program of ρ_{hi} in *m*-Healthcare emergency.

Mobile healthcare's primary objective is to diagnose and monitor illnesses timelier i.e., more actionable data about health. Most patients now use home tracking for diagnosis for a few days; no monitoring is required in the hospital environment. *m*-health is considered the cornerstone for e-health. Through *m*-healthcare-based mobile technology, information of personal health is provided to various medical consumers. It can make regions, individuals and/or medical users more accessible. Lu et al.'s (2013) system has security flaws in mutual authentication and patient anonymity. Keeping in mind the end goal is to settle those issues and extra elevation of the calculation efficiency.

With the advent of 5G technology and use of IoT with 5G, we devised a new framework called as 5G-IoT. The 5G-IoT facing the challenge of privacy and security during data transmission. Hence, quantum walks (QWs) model is proposed to develop efficient cryptosystem wherein new S-box is implemented for block cipher computation under 5G-IoT environment (Abd El-Latif et al. 2020b). The combination of CAQWs and S-box is utilized for secure transmission of video data with efficient efficacy and security. In Abd El-Latif et al. (2020c), an end-to-end secure data transmission technique using QWs is proposed to resist the potential attacks on IoT systems for image data. The QWs are utilized to generate pseudo-random numbers (PRNG) and design permutation boxes to encrypt input image blockwise. Furthermore, a complex chaotic circuit based on diode bridge circuit is developed for image encryption in Tsafack et al. (2020b). This chaotic-based encryption adopts the S-Box and PRNG generation to secure the images. Moreover, performance is validated on time complexity, entropy, and rate of change of pixel, among others.

The significance of the conformable chaotic map (CCM) is to improve the appearance encryption scheme based on it. Compared with custom classic ordinary chaotic maps such as the Logistic Map and the Tent Map, this CCM indicated that chaotic map establishes numerous improved chaotic possessions for encryption, inferred by a much larger maximal polynomial formula. In this work, our aim is to devise a new effective *m*-Healthcare emergency system using conformable chaotic maps. By using our system, the authentication system can give patients anonymity as well as accomplish mutual authentication by taking minimal computation cost. This article's main contributions are devising a new effective *m*-Healthcare emergency system with the efficient security of the unusual *m*-Healthcare emergency system, and enhancing the efficiency of an unusual *m*-Healthcare emergency system using conformable chaotic maps.

The rest of this article is structured as follows. We have presented the related backgrounds such as conformable chaotic maps, the system and security model in Sect. 2. Our proposed new effective *m*-Healthcare emergency system using conformable chaotic maps under cloud computing environment is outlined in Sect. 3. The security review and an execution inquiry are presented in Sect. 4. Finally, we conclude this paper in Sect. 5.

2 Related works

This part of investigation includes an existing literature, brief introduction of a few algorithms used by our new protocol, Conformable Chebyshev polynomial, conformable chaotic maps, system model, security investigation model and a list of notations used throughout this paper.

A biometric such as face and iris is adopted to assess human diseases as well as healthcare monitoring. In El-Latif et al. (2019), healthcare monitoring prototype is proposed by using biometric to provide healthcare assistance to the patient. The patient biometrics, i.e., face and iris, are stored in the cloud, which are verified at the time of healthcare request. This prototype offers efficient healthcare monitoring by employing multibiometrics fusion infrastructure based on face and iris features extractor.

Subsequently, quantum computing becomes the challenge to existing security algorithms due to its ability to design contemporary cryptographic algorithms. In Abd EL-Latif et al. (2020a), IoT-based healthcare framework is proposed to preserve the privacy of patients' by new encryption technique wherein quantum walks is utilized to encrypt or decrypt the image data. The presented cryptosystem consists of substitution phase and permutation phase, which work independently. In Abd-El-Atty et al. (2020), image steganography model based on controlled alternate quantum walks (CAQWs) is presented for E-healthcare system under cloud infrastructure wherein no need of secret images and carrier pre or post encryption. The secret image is implanted on cover image by applying CAQWs. The CAQWs is utilized to identify the position of pixels related to carrier image for secret bits filling.

A sustainable healthcare system for IoT is presented in Abou-Nassar et al. (2020) wherein Blockchain is applied for trustworthy communication. This framework preserves the privacy related to patients' sensitive data. Moreover, it enhances encryption, improves security, and ensures integrity and confidentiality of patients' data. In Tsafack et al. (2020a), a secure transmission of medical data (images) via Internet of Healthcare Things (IoHT) is presented. New Chaotic Map is utilized, which is based on 2-D trigonometric map satisfying the chaotic dynamics. The construction of the proposed cryptosystem comprises the sequences of these maps. The performance evaluation shows the system is more secure and suitable for IoHT to secure medical data.

In healthcare monitoring, detection of diseases plays a vital role in diagnosis. Deep neural networks are investigated to detect myocardial infarction (MI) from Electrocardiogram (ECG) data because manually it is difficult for the doctors to accurately detect and start the diagnosis. Therefore, convolution neural networks (CNN) are applied to detect MI in urban healthcare under smart cities project (Alghamdi et al. 2020). The authors presented the two transfer learning based model using VGG-Net; namely VGG-MI1 and VGG-MI2, which detect MI with an accuracy of 99.02% and 99.22%, respectively.

2.1 Chebyshev chaotic transforms

Basically, we review Chebyshev sequential Polynomials (CP) (Mason and Handscomb 2003) and evaluate their functionality in this section. CP $\mathcal{T}_{r}(z)$ is a polynomial of n-degree in the variant z. Let $z \in [-1, 1]$ be the version, and let n be an integer. In general, CP stated as follows:

$$\mathcal{T}_n(z) = \cos(n\arccos(z)),$$

$$\mathcal{T}_0(z) = 1$$

$$\mathcal{T}_1(z) = z$$

$$\mathcal{T}_n(z) = 2z\mathcal{T}_{n-1}(z) - \mathcal{T}_{n-2}(z); n \geq 2$$

In this case, the functional $\arccos(z)$ and $\cos(z)$ are represented as $\arccos : [-1, 1] \to [0, \pi]$ and $\cos : \mathrm{R} \to [-1, 1]$.

There are two main properties of CP (Bergamo et al. 2005; Han and Chang 2009; Zhang 2008; Chen et al. 2012; Meshram et al. 2019a,b): chaotic properties and bisection-group properties.

(1) The chaotic possessions: The CP transform demarcated as $\mathcal{T}_r : [-1, 1] \to [-1, 1]$ with degree $n > 1$ is a chaotic transform connected the functional (invariant density) $f^*(z) = \frac{1}{(\pi\sqrt{1-z^2})}$, for some confident Lyapunov proponent $\lambda = 1$.

(2) The possessions of what is calling semigroup satisfy the following equalities:
$\mathcal{T}_{\omega}(\mathcal{T}_{\ell}(z)) = \cos(\omega\cos^{-1}$ $(\cos(\ell\cos^{-1}(z)))) = \cos(\omega\ell\cos^{-1}(z)) = \mathcal{T}_{\ell\omega}(z) = \mathcal{T}_{\ell}(\mathcal{T}_{\omega}(z))$, where ω and ℓ are positive integers and $z[-1, 1]$.

Chebyshev polynomials have two tests that in polynomial time consider handling:

(1) The discrete log's (DL) assignment is to find the integer ω with the end goal $\mathcal{T}_{\omega}(z) = y$ given two components z and y.
(2) Because of three components z, $\mathcal{T}_{\omega}(z)$, and $\mathcal{T}_{\ell}(z)$, the Diffie–Hellman problem (DHP) assignment is to measure the $\mathcal{T}_{\omega\ell}(z)$ element.

2.2 Conformable chaotic maps (CCM)

The conformable calculus (CC) is formerly stated as a conformable fractional calculus (Anderson et al. 1810). Essentially, CC receives the subsequent preparation:

Suppose the fractional (arbitrary) is given as $\alpha \in [0, 1]$. An operator δ^{α} is conformable differential if and only if δ^0 is the self-operator and δ^1 is the traditional difference operative. Specifically, δ^{α} is conformable if and only if for differentiable utility $\vartheta = \vartheta\ (x)$,

$$\delta^0\vartheta(x) = \vartheta(x), \delta^1\vartheta(x) = \vartheta'(x).$$

Newly, Anderson et al. (1810) presented a novel formulation of CC founded by the control theory to designate the performance of proportional-differentiation controller conforming to error function. The prescription has the following classification.

Definition 2.1 Assume that $\alpha \in [0, 1]$, then CC has in the subsequent recognized

$$\delta^{\alpha}\vartheta(x) = \mu_1(\alpha, x)\vartheta(x) + \mu_0(\alpha, x)\vartheta'(x),$$

where the functions μ_1 and μ_0 attain the boundaries

$$\lim_{\alpha\to 0}\mu_1(\alpha, x) = 1, \lim_{\alpha\to 1}\mu_1(\alpha, x) = 0,$$

$$\lim_{\alpha\to 0}\mu_0(\alpha, x) = 0, \lim_{\alpha\to 1}\mu_0(\alpha, x) = 1.$$

To attain the overhead description, we shall deliberate $\mu_1(\alpha, x) = (1-\alpha)x^{\alpha}$ and $\mu_0(\alpha, x) = \alpha x^{1-\alpha}$, or $\mu_1(\alpha, x) = \frac{(1-\alpha)}{\Gamma(1+\alpha)}$ and $\mu_0(\alpha, x) = \frac{\alpha}{\Gamma(1+\alpha)}$ where $\delta^{\alpha}\vartheta(x)$ is named the conformable differential operator for the function $\vartheta(x)$. Consequently, μ_1, μ_0 are the fractional tuning connections of the function ϑ and its derivative, respectively.

By applying the concept of CC to generalize the polynomial $\mathcal{T}_n(z)$, we obtain the following construction:

Since $\mathcal{T}'_n(z) = 2n\mathcal{T}_{n-1}(z)$, then $\delta^{\alpha}\mathcal{T}_n(z)$ has the following formal form:

$$\mathcal{T}_n{}^{\alpha}(z) := \delta^{\alpha}\mathcal{T}_n(z) = \mu_1(\alpha, z)\mathcal{T}_n(z) + \mu_0(\alpha, z)\mathcal{T}'_n(z) \quad (1)$$

Equation (1) can be rewritten as shown below:

$$\mathcal{T}_n{}^{\alpha}(z) = \mu_1(\alpha, z)\mathcal{T}_n(z) + 2n\mu_0(\alpha, z) * \omega(z)\mathcal{T}_{n-1}(z), \quad (2)$$

where $\omega(z) = 1 + 2z + (4z^2 - 1) + \cdots + (n-1)$-times. Equation (2) is called the Conformable Chebyshev Polynomials (CCP). Figure 2 shows the dynamic plot of the presented CCP. The formula that is more frequent can be seen in the following result:

Proposition 2.1 *The CCP fulfills the frequent associations:*

$$\mathcal{T}_n{}^{\alpha}(z) = [2z\mu_1(\alpha, z) + 2n\mu_0(\alpha, z) * \omega(z)]\mathcal{T}_{n-1}(z) - \mu_1(\alpha, z)\mathcal{T}_{n-2}(z). \quad (3)$$

Proof Joining (2) with the frequent formula $\mathcal{T}_n(z) = 2z\mathcal{T}_{n-1}(z) - \mathcal{T}_{n-2}(z); n \geq 2$, we get:

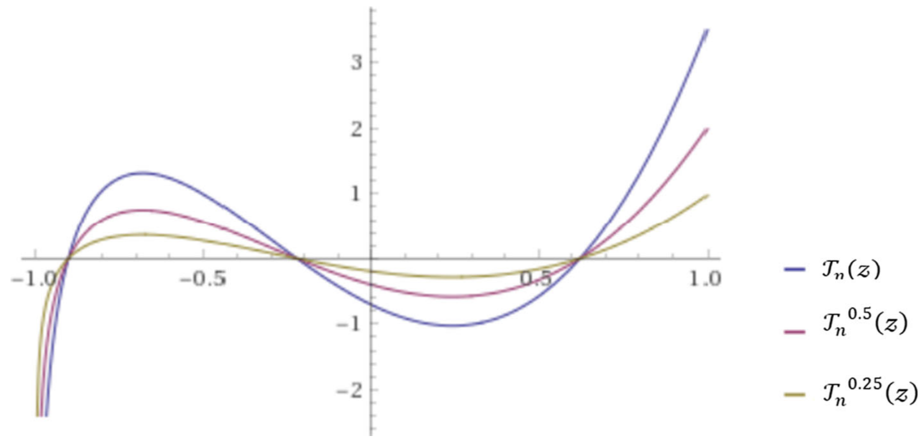

Fig. 2 CCP for diverse tenets of α with $\mu_1(\alpha, x) = \frac{(1-\alpha)}{\Gamma(1+\alpha)}$ and $\mu_0(\alpha, x) = \frac{\alpha}{\Gamma(1+\alpha)}$

$$\begin{aligned}\mathcal{T}_n{}^{\alpha}(\varkappa) &= \mu_1(\alpha,\varkappa)\mathcal{T}_n(\varkappa) + 2n\mu_0(\alpha,\varkappa) * \omega(\varkappa)\mathcal{T}_{n-1}(\varkappa)\\ &= \mu_1(\alpha,\varkappa)[2\varkappa\mathcal{T}_{n-1}(\varkappa) - \mathcal{T}_{n-2}(\varkappa)] + 2n\mu_0(\alpha,\varkappa)*\\ &\quad \omega(\varkappa)\mathcal{T}_{n-1}(\varkappa)\\ &= [2\varkappa\mu_1(\alpha,\varkappa)+2n\mu_0(\alpha,\varkappa) * \omega(\varkappa)]\mathcal{T}_{n-1}(\varkappa)\\ &\quad - \mu_1(\alpha,\varkappa)\mathcal{T}_{n-2}(\varkappa).\end{aligned}$$

Note when $\alpha \to 0$, we have the main ordinary result, which can be seen in Zhang (2008).

Proposition 2.2 *The semigroup possessions holds for CCP positioned in interval* $(-\propto, \propto)$.

Proof. Let $H = z\mu_1(\alpha,\varkappa) + n\mu_0(\alpha,\varkappa) * \omega(\varkappa)z\mu_1(\alpha,\varkappa)$.
By Proposition 2.1, we obtain:

$$\mathcal{T}_{n+2}{}^{\alpha}(\varkappa) = 2H\mathcal{T}_{n+1}(\varkappa) - \mu_1(\alpha,\varkappa)\mathcal{T}_n(\varkappa)$$

The overhead formulation suggests a modification equation (disconnected equation) which has a typical principle:

$$\sigma^2 - 2H\sigma + \mu_1 = 0$$

satisfying the relations:

$$\sigma_1 + \sigma_2 = 2H, \sigma_1\sigma_2 = \mu_1, \sigma_{1,2} = H \pm \sqrt{H^2 - \mu_1}.$$

So, computation yields:

$$\begin{aligned}\mathcal{T}_n{}^{\alpha}(\varkappa) &= (\sigma_1{}^n + \sigma_2{}^n)/2\\ &= \frac{\left(H + \sqrt{H^2 - \mu_1}\right)^n + \left(H - \sqrt{H^2 - \mu_1}\right)^n}{2}\\ &= \sum_{m=0}^{[n/2]} \binom{n}{m} H^{n-2m} (H^2 - \mu_1)^m\end{aligned}$$

From the proof in Zhang (2008) on the overhead summation, we get:

$$\mathcal{T}_k{}^{\alpha}(\mathcal{T}_n{}^{\alpha}(\varkappa)) = (\tau_1{}^k + \tau_2{}^k)/2$$

$$\tau_1 + \tau_2 = 2\mathcal{T}_n{}^{\alpha}(\varkappa), \sigma_1\sigma_2 = \mu_1.$$

Hence, we have the following important relation:

$$\mathcal{T}_k{}^{\alpha}(\mathcal{T}_n{}^{\alpha}(\varkappa)) = \mathcal{T}_n{}^{\alpha}(\mathcal{T}_k{}^{\alpha}(\varkappa)) = \mathcal{T}_{kn}{}^{\alpha}(\varkappa).$$

Note that, when $\alpha \to 0$, we have the original case of Proposition 2.2, which was established in Zhang (2008).

In this place, we note that the DL and DHP assignments for the CCP approximately occur.

2.3 System model

We concentrated on the security in the cloud setting in this research work. Security can be given in various ways. In our strategy, we provide *m*-healthcare service with security. We have different medical patients who have distinct delicate illnesses such as heart attack, emergency condition, etc. These patients need automatic assistance whenever required from emergency centers. Every medical patient/user can be linked to the healthcare station from the architecture design.

Every 5 min a day, every medical patient/user is monitored by the healthcare station. Every medical patient/user can have a definite report from the healthcare center. If the person has any health problem from observing every 5 min, some modifications will automatically happen in the ordinary report. In this scenario, from the doctor's advice, prescription and instruction, the healthcare center can interact with specific physicians and give a key to the precise medical customer. Medical clients use the fresh key to encrypt the message and send it to the healthcare center. After obtaining the data, the healthcare center defines the precise issue of the patient, with the assistance of the specific physicians. The emergency center is instantly informed by the dedicated physicians and healthcare station. The emergency vehicle will reach the medical patients/user in less time. The system architecture design under our consideration as presented in Fig. 3. According to the presented scheme shown in Fig. 3, we recognize that there is a Trusted Center ($\mathcal{TC}$) and a collection $\mathcal{P} =$

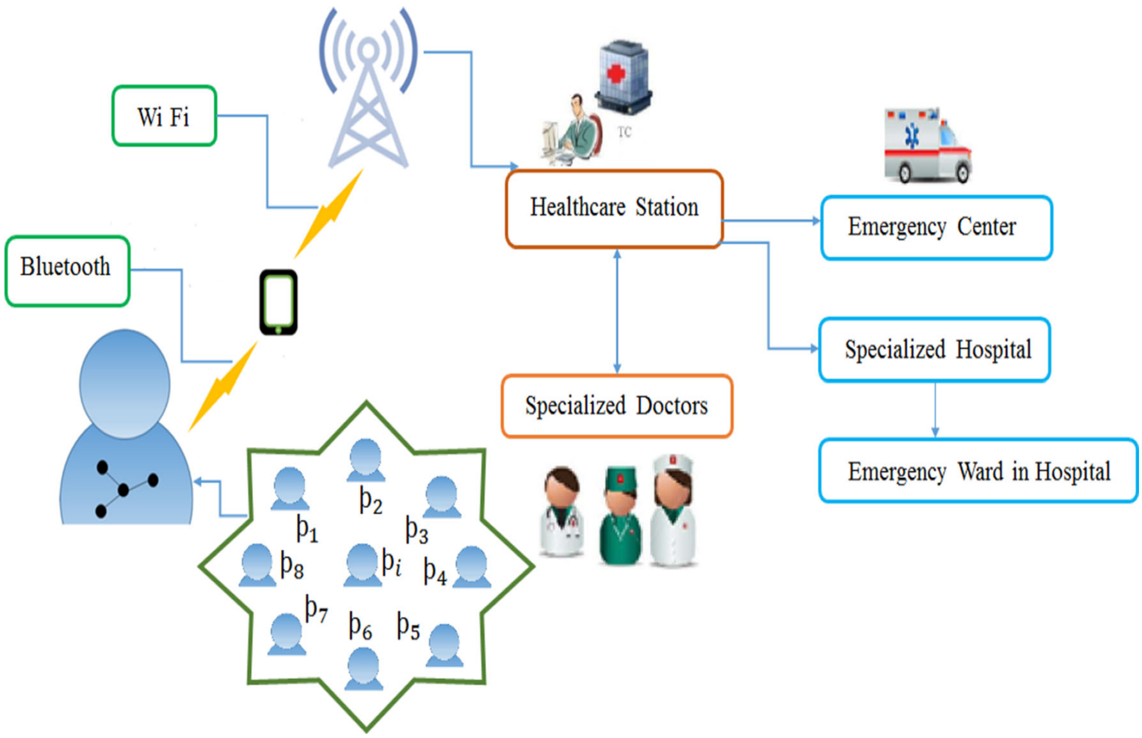

Fig. 3 System model under consideration

$(\phi_1, \phi_2, \ldots, \phi_\kappa)$ of κ patients. The responsibility of $\mathcal{TC}$ is to manage the entire m-Healthcare system, set up system's legitimately and prepare the appropriate body sensor nodes for the κ patients. Characteristically, at the medical centers, $\mathcal{TC}$ would be a competent, and reliable individual. By using m-Healthcare system, the focus of the medical faculties can provide improved quality healthcare for every patient with the help of the individual BSN and SP that can receive and notify the healthcare personnel. Here, the patients are considered mobile and are not exactly the same as home or hospital in-bed patients (see Meshram et al. 2017a,b,2012).

Assume an emergency happens in the case of a patient ϕ_4, as shown in Fig. 3. Let us say that on the way of home, he has a sudden heart attack and he falls unconscious to the ground. Temporarily, $\mathcal{TC}$ recurrently observes the health condition of ambient ϕ_4, $\mathcal{TC}$ gets the abnormal ρ_{hi} interpretations of ϕ_4 and suggests that there has been an emergency. $\mathcal{TC}$ sends medical personnel and an ambulance to the emergency region instantly. Already the ambulance comes, high-powered ρ_{hi} is needed by the medical employee in order to continuously pursue ϕ_4. However, it may not be appropriate to assist the high-power ρ_{hi} handling and interaction with the calculated energy of the ubiquitous SP. In this circumstance, new patients, for example, ϕ_1, ϕ_2 or ϕ_3 will share the assets accessible on their SP's in order to assist ϕ_4 in preparing and communicating the high power ρ_{hi}.

2.4 Security investigation model

In an emergency circumstance in m-Healthcare, the opportunistic computing component can certainly improve the unwavering quality of the high-power ρ_{hi} handling and communication method. Nevertheless, even in emergency conditions, patients will not need their ρ_{hi} to be subjected to all other neighboring patients. Rather, together with other patients with comparable side impacts, they may just want to nurture this kind of membership and brotherhood with ρ_{hi}-revelation. Lu et al. subsequently created a two-stage Security Ingress Control Proposal for Opportunistic Computing (Lu et al. 2013) for high-dependence ρ_{hi}, m-Healthcare emergency management and communication (see Fig. 4). The two stages are briefly described below:

1. *Stage-I ingress control* In order to bring opportunistic computing into practice at this stage, all the SPs involvement is needed to have comparable medical preparation implemented so that they can cooperate with each other in preparing and communicating the ρ_{hi}. Deprived of the fundamental training, a going by individual who is not a patient will not be a perfect assistant despite the fact that he/she has a SP with sufficient power. Thus, ingress control is necessary in Stage-I security.
2. *Stage-II ingress control* At this step, patients with comparable side impacts are allowed to participate in opportunistic computation and to assist in ρ_{hi}

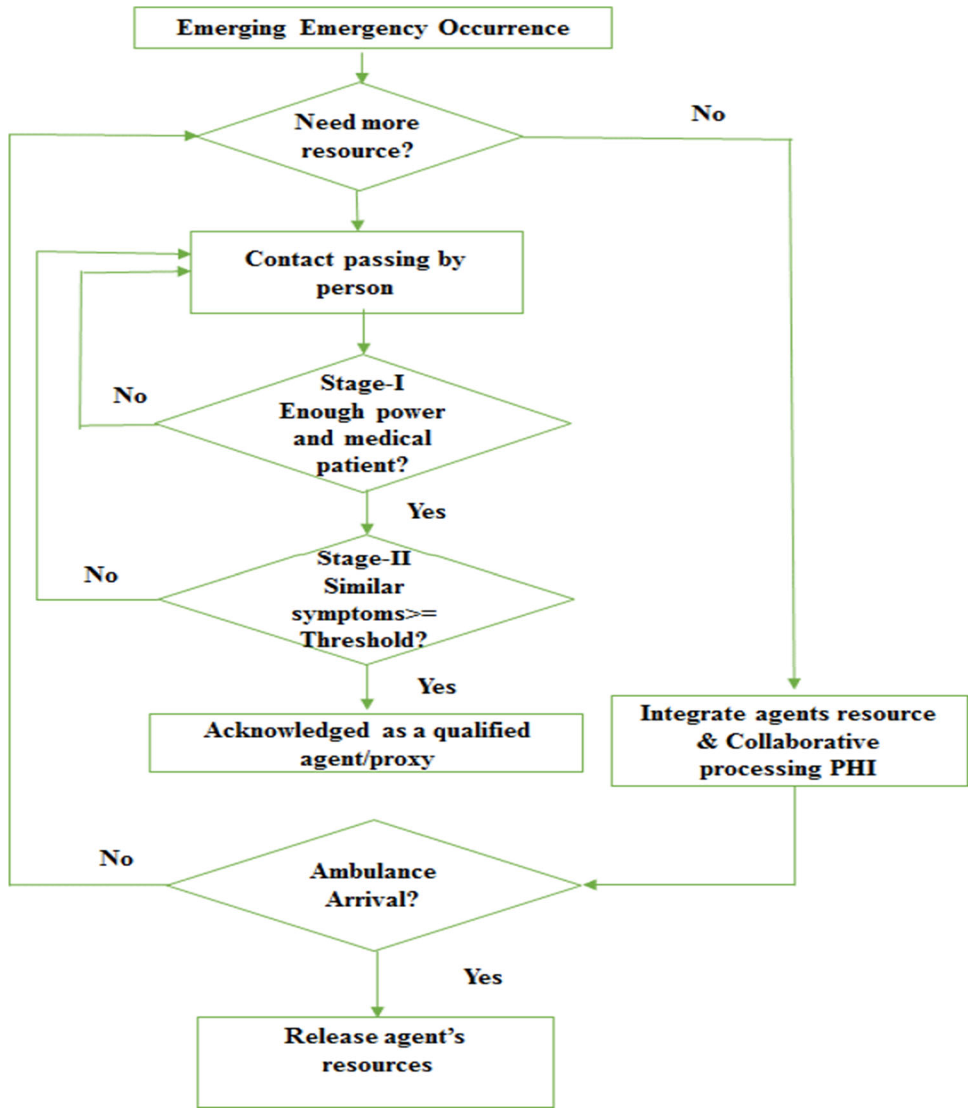

Fig. 4 Two-stage secrecy Ingres control for *m*-Healthcare emerging emergency utilizing opportunistic computing

operation. If it is not taking too many problems, use a $\mathscr{th}$ threshold that can function as a patient self-control restriction to notice that nearby. The $\mathscr{th}$ threshold is set high to restrict disclosure of privacy at the time of emergency that occurs in a region where communication activity is high. On the other hand, $\mathscr{th}$ must be low if there is low movement around that area. Along these lines, the high-dependability ρ_{hi} preparation and communication means can be guaranteed.

3 Proposed mobile-healthcare emerging emergency medical system

In this section, we introduced an efficient mobile-healthcare emerging emergency medical system using conformable chaotic maps. Our novel system contains two components: initialization of the system and control of patient-centered security entry for *m*-Healthcare medical emergency.

3.1 System initialization

In *m*-Healthcare system based on single-authority, we expect that the trusted center $(\mathcal{TC})$ situated at the health-care center to bootstrap the entire system. In the first place, the $\mathcal{TC}$ choices a secure $E_n(.)$ and $\mathscr{s}$, a random integer as the master secret key. Additionally, $\mathcal{TC}$ chooses arbitrary numbers $(\mathscr{z}_1, \mathscr{z}_2)$ and analyzes$\mathcal{T}^{\alpha}_{\mathscr{s}}(\mathscr{z}_1)(\bmod n)$, $\mathcal{T}^{\alpha}_{\mathscr{s}}(\mathscr{z}_2)(\bmod n)$. The $\mathcal{TC}$ holds onto $\mathscr{s}$ in private and distributes the parameters which are public $(n, E_n(), \mathscr{h}(\cdot))$.

Let us assume that there is aggregate of n indexes or side effect characters considered in *m*-Healthcare system. $\mathcal{TC}$ selects a binary vector $\overrightarrow{\boldsymbol{\beta}} = (\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \ldots, \boldsymbol{\beta}_n)$ for every patient in the n-dimensional index character space. For each $\boldsymbol{\beta}_i \in \overrightarrow{\boldsymbol{\beta}}$, we have $\boldsymbol{\beta}_i = 1$ if the patient has the relating side effect character, and $\boldsymbol{\beta}_i = 0$, otherwise. At that point, the physicians at the healthcare center lead the medical checks for every patient $\phi_i \in \mathcal{P}$ and create ϕ_i's individual health profile $\overrightarrow{\boldsymbol{\beta}} = (\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \ldots, \boldsymbol{\beta}_n)$ when ϕ_i lists in the healthcare center. Then, $\mathcal{TC}$ will perform the following steps:

1. As indicated by the patient ϕ_i's individual health record $\overrightarrow{\boldsymbol{\beta}}$, $\mathcal{TC}$ picks the best possible body device knobs to build up ϕ_i's own BSN and installs the vital medical programming in ϕ_i's SP.
2. $\mathcal{TC}$chooses arbitrary integers (ϑ_i, μ_i) and calculates the secret values $\mathcal{T}^{\alpha}_{\mathscr{s}\vartheta_i}(\mathscr{z}_1)(\bmod\, \mathscr{n})$, $\mathcal{T}^{\alpha}_{\vartheta_i}(\mathscr{z}_1)(\bmod\, \mathscr{n})$, and $\mathcal{T}^{\alpha}_{\mathscr{s}\mu_i}(\mathscr{z}_2)(\bmod\, \mathscr{n})$ for every patient, ϕ_i.
3. Then, $\mathcal{TC}$ sends $\{\mu_i, \mathcal{T}^{\alpha}_{\mathscr{s}\vartheta_i}(\mathscr{z}_1)(\bmod\, \mathscr{n}), \mathcal{T}^{\alpha}_{\vartheta_i}(\mathscr{z}_1)(\bmod\, \mathscr{n}), \mathcal{T}^{\alpha}_{\mathscr{s}\mu_i}(\bmod\, \mathscr{n})\}$ for each ϕ_i by incomes of a locked station.

By consuming the secret standards $[\mathcal{T}^{\alpha}_{\vartheta_i}(\mathscr{z}_1)(\bmod\, \mathscr{n}), \mathcal{T}^{\alpha}_{\mathscr{s}\vartheta_i}(\mathscr{z}_1)(\bmod\, \mathscr{n})]$ and individual BSN, ϕ_i can carefully report his/her ρ_{hi} to the healthcare center and then the subsequent steps are achieved:

1. The patient ϕ_i uses his/her SP to choose a random integer η_i. Henceforth, with the current time $\mathcal{PD}$, ϕ_i can develop the session key $\boldsymbol{\kappa}_i = \mathscr{h}(\mathcal{T}^{\alpha}_{\eta_i}(\mathcal{T}^{\alpha}_{\mathscr{s}\vartheta_i}(\mathscr{z}_1))(\bmod\, \mathscr{n})) \parallel \mathcal{PD})$ for the day. At that point U_i disperses the session key $\boldsymbol{\kappa}_i$ to his/her individual BSN.
2. ϕ_i's BSN receives the basic ρ_{hi} statistics, in particular $\omega\rho_{hi}$, and records the translated value $E_n(\boldsymbol{\kappa}_i, \omega\rho_{hi} \parallel \mathcal{PD})$ to the SP with Bluetooth innovation once at regular intervals.
3. After accepting the encrypted $E_n(\boldsymbol{\kappa}_i, \omega\rho_{hi} \parallel \mathcal{PD})$, the SP utilizes $\boldsymbol{\kappa}_i$ to recover $\omega\rho_{hi}$ from $E_n(\boldsymbol{\kappa}_i, \omega\rho_{hi} \parallel \mathcal{PD})$. At that point, the SP calculates $\mathcal{T}^{\alpha}_{\eta_i}(\mathcal{T}^{\alpha}_{\vartheta_i}(\mathscr{z}_1))(\bmod\, \mathscr{n})$ and utilizes 4G innovation to communicate the handled ρ_{hi} to the healthcare center as of $\mathcal{T}^{\alpha}_{\eta_i}(\mathcal{T}^{\alpha}_{\vartheta_i}(\mathscr{z}_1))(\bmod\, \mathscr{n}) \parallel \mathcal{PD} \parallel E_n(\boldsymbol{\kappa}_i, \phi_i \parallel \rho_{hi} \parallel \mathcal{PD})$.
4. After accepting$\mathcal{T}^{\alpha}_{\eta_i}(\mathcal{T}^{\alpha}_{\vartheta_i}(\mathscr{z}_1))(\bmod\, \mathscr{n}) \parallel \mathcal{PD} \parallel E_n(\boldsymbol{\kappa}_i, \phi_i \parallel \rho_{hi} \parallel \mathcal{PD})$, $\mathcal{TC}$ initially utilizes the secret key $\mathscr{s}$ to calculate $\mathscr{h}(\mathcal{T}^{\alpha}_{\mathscr{s}}(\mathcal{T}^{\alpha}_{\eta_i\vartheta_i}(\mathscr{z}_1))(\bmod\, \mathscr{n}))$ and utilize it to calculate the session key $\boldsymbol{\kappa}_i = \mathscr{h}(\mathcal{T}^{\alpha}_{\mathscr{s}}(\mathcal{T}^{\alpha}_{\eta_i\vartheta_i}(\mathscr{z}_1))(\bmod\, \mathscr{n})) \parallel \mathcal{PD})$. At that point, $\mathcal{TC}$ utilizes the session key $\boldsymbol{\kappa}_i$ to recover $\phi_i \parallel \rho_{hi} \parallel \mathcal{PD}$ from $E_n(\boldsymbol{\kappa}_i, \phi_i \parallel \rho_{hi} \parallel \mathcal{PD})$. From that point onward, $\mathcal{TC}$ sends ρ_{hi} to the physicians for interpretation if the recovered $\mathcal{PD}$ is right.

Moreover, the initialization of the system for the proposed emergency system is presented in Algorithm 1 and control of patient-centered security entry is discussed stepwise nicely in Sect. 3.

Algorithm 1: System Initialization

---

1 $\mathcal{TC}$ chooses, secure $E_n(.)$ and master secret key, $\mathscr{s}$. Also, $\mathcal{TC}$ chooses arbitrary numbers $(\mathscr{z}_1, \mathscr{z}_2)$ and analyses $\mathcal{T}^{\alpha}_{\mathscr{s}}(\mathscr{z}_1)(\bmod n)$, $\mathcal{T}^{\alpha}_{\mathscr{s}}(\mathscr{z}_2)(\bmod\, n)$. $\mathcal{TC}$ keeps $\mathscr{s}$ and distributes the public parameters $(n, E_n(), \mathscr{h}(\cdot))$

2 If there is aggregate of n indexes or side effect characters considered in m-Healthcare system. Then, $\mathcal{TC}$ selects a binary vector $\overrightarrow{\boldsymbol{\beta}} = (\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \ldots, \boldsymbol{\beta}_n)$ for every patient in the n-dimensional index character space. For each $\boldsymbol{\beta}_i \in \overrightarrow{\boldsymbol{\beta}}$, if $\boldsymbol{\beta}_i = 1$, the patient with side effect character, and $\boldsymbol{\beta}_i = 0$, otherwise

Hence, medical checkup is initiated by the physicians for patients $\phi_i \in \mathcal{P}$ and creates ϕ_i's individual health profile $\overrightarrow{\boldsymbol{\beta}} = (\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \ldots, \boldsymbol{\beta}_n)$. Afterward, $\mathcal{TC}$ performs the following steps:

2.1 As per ϕ_i's individual health record $\overrightarrow{\boldsymbol{\beta}}$, $\mathcal{TC}$ chooses suitable body device knobs for building ϕ_i's own BSN and vital medical programming is installed in ϕ_i's SP.

2.2 $\mathcal{TC}$ chooses (ϑ_i, μ_i) and computes $\mathcal{T}^{\alpha}_{\mathscr{s}\vartheta_i}(\mathscr{z}_1)(\bmod\, \mathscr{n})$,$\mathcal{T}^{\alpha}_{\vartheta_i}(\mathscr{z}_1)(\bmod\, \mathscr{n})$, and $\mathcal{T}^{\alpha}_{\mathscr{s}\mu_i}(\mathscr{z}_2)(\bmod\, \mathscr{n})$, the secret values for patients, ϕ_i.

2.3 $\mathcal{TC}$ sends $\{\mu_i, \mathcal{T}^{\alpha}_{\mathscr{s}\vartheta_i}(\mathscr{z}_1)(\bmod\, \mathscr{n}), \mathcal{T}^{\alpha}_{\vartheta_i}(\mathscr{z}_1)(\bmod\, \mathscr{n}), \mathcal{T}^{\alpha}_{\mathscr{s}\mu_i}(\bmod\, \mathscr{n})\}$ for eachϕ_i.

3 If secret standards $[\mathcal{T}^{\alpha}_{\vartheta_i}(\mathscr{z}_1)(\bmod\, \mathscr{n}), \mathcal{T}^{\alpha}_{\mathscr{s}\vartheta_i}(\mathscr{z}_1)(\bmod\, \mathscr{n})]$ are consumed and individual BSN observed, then ϕ_i reports ρ_{hi} to healthcare center. The following steps are performed:

3.1 ϕ_i selects η_i. ϕ_i develops the session key $\boldsymbol{\kappa}_i = \mathscr{h}(\mathcal{T}^{\alpha}_{\eta_i}(\mathcal{T}^{\alpha}_{\mathscr{s}\vartheta_i}(\mathscr{z}_1))(\bmod\, \mathscr{n})) \parallel \mathcal{PD})$ based on the current time $\mathcal{PD}$. Hence, U_i scatters $\boldsymbol{\kappa}_i$ to individual BSN.

3.2 ϕ_i' s BSN receives ρ_{hi}, i.e., $\omega\rho_{hi}$, and records $E_n(\boldsymbol{\kappa}_i, \omega\rho_{hi} \parallel \mathcal{PD})$ to SP.

3.3 After that, the SP utilizes $\boldsymbol{\kappa}_i$ to recover $\omega\rho_{hi}$ from $E_n(\boldsymbol{\kappa}_i, \omega\rho_{hi} \parallel \mathcal{PD})$. Here, SP computes $\mathcal{T}^{\alpha}_{\eta_i}(\mathcal{T}^{\alpha}_{\vartheta_i}(\mathscr{z}_1))(\bmod\, \mathscr{n})$ and 4G is used to send ρ_{hi} to the healthcare center as $\mathcal{T}^{\alpha}_{\eta_i}(\mathcal{T}^{\alpha}_{\vartheta_i}(\mathscr{z}_1))(\bmod\, \mathscr{n}) \parallel \mathcal{PD} \parallel E_n(\boldsymbol{\kappa}_i, \phi_i \parallel \rho_{hi} \parallel \mathcal{PD})$.

3.4 After accepting $\mathcal{T}^{\alpha}_{\eta_i}\left(\mathcal{T}^{\alpha}_{\vartheta_i}(\mathscr{z}_1)\right)(\bmod\, \mathscr{n}) \parallel \mathcal{PD} \parallel E_n(\boldsymbol{\kappa}_i, \phi_i \parallel \rho_{hi} \parallel \mathcal{PD})$, $\mathcal{TC}$ uses $\mathscr{s}$ to compute $\mathscr{h}(\mathcal{T}^{\alpha}_{\mathscr{s}}(\mathcal{T}^{\alpha}_{\eta_i\vartheta_i}(\mathscr{z}_1))(\bmod\, \mathscr{n}))$ and henceforth $\boldsymbol{\kappa}_i = \mathscr{h}(\mathcal{T}^{\alpha}_{\mathscr{s}}(\mathcal{T}^{\alpha}_{\eta_i\vartheta_i}(\mathscr{z}_1))(\bmod\, \mathscr{n})) \parallel \mathcal{PD})$ is computed. Afterword, $\mathcal{TC}$ utilizes $\boldsymbol{\kappa}_i$ to extract $\phi_i \parallel \rho_{hi} \parallel \mathcal{PD}$ from$E_n(\boldsymbol{\kappa}_i, \phi_i \parallel \rho_{hi} \parallel \mathcal{PD})$. Later, $\mathcal{TC}$ sends ρ_{hi} to the physicians for analysis if the extracted $\mathcal{PD}$ is right.

3.2 *m*-Healthcare emergency based on Patient-centric confidentiality access control

Similar to (Lu et al. 2013), if an emergency situation occurs to a patient ϕ_i, the observing healthcare center immediately classifies the emergency. Then, it quickly dispatches medical staffs along with ambulance to attend the emergency. Before the entrance of ambulance, the medical control requires high-force ρ_{hi} to observe ϕ_i progressively. However, the energy of ϕ_i's SP might be too low to help the high-force ρ_{hi} preparation and transmission. Assume that a different patient ϕ_j, who is cruising by, has a SP with enough energy to aid management and communicating ϕ_i's high-power ρ_{hi} information. The accompanying patient-centric security access control is then executed to limit the ρ_{hi} protection exposure under opportunistic computing.

3.2.1 Stage-I ingress control

The main objective of Stage-I ingress control is to catch further patients and collect more energy to assist with the emergency. Figure 5 shows that patients ϕ_i and ϕ_j will implement the accompanying advances:

1. ϕ_i initially utilizes his/her SP to create an arbitrary integer ω_i and calculates $\mathbb{M}_1 \equiv \mathcal{T}^{\alpha}_{\omega_i}(\mathcal{T}^{\alpha}_{\jmath\mu_i}(\imath_2))(\bmod\, \varkappa)$. At that point, ϕ_i sends $\{\mathbb{M}_1\}$ to ϕ_j when ϕ_j goes by the emergency location.
2. After accepting $\{\mathbb{M}_1\}$, ϕ_j likewise creates an arbitrary integer ω_j and calculates
$$\mathbb{k}_{ij} \equiv \mathcal{T}^{\alpha}_{\mu_j\omega_j}(\mathbb{M}_1)(\bmod \varkappa),$$
$$\mathbb{M}_2 \equiv \mathcal{T}^{\alpha}_{\omega_i}\left(\mathcal{T}^{\alpha}_{\jmath\mu_i}(\imath_2)\right)(\bmod \varkappa),$$
$$Auth = h\left(\mathbb{M}_1 \parallel \mathbb{k}_{ij}\right).$$
3. ϕ_j sends back $\{Auth, \mathbb{M}_2\}$ to ϕ_i.
4. Subsequent to getting $\{Auth, \mathbb{M}_2\}$, U_i calculates $\mathbb{k}'_{ij} \equiv \mathcal{T}^{\alpha}_{\mu_i\omega_i}(\mathbb{M}_2)(\bmod\, \varkappa)$ and checks $Auth? = h(\mathbb{M}_1 \parallel \mathbb{k}'_{ij})$. If it holds, ϕ_j is validated as a patient and passes the stage-I ingress control. At that point, ϕ_i calculates $Auth' = h(\mathbb{M}_2 \parallel \mathbb{k}_{ij})$ and sends $\{Auth'\}$ to ϕ_j. Else, ϕ_i rejects the session.
5. Finally, ϕ_j utilizes the acquired message $\{Auth'\}$ to check $Auth'? = h(\mathbb{M}_2 \parallel \mathbb{k}_{ij})$. If it holds, ϕ_i likewise is authenticated as a patient; the mutual authentication among ϕ_i and ϕ_j is accomplished. Else, ϕ_j rejects the session.

3.2.2 Stage-II ingress control

After $\mathcal{P}_j$ permits the stage-I ingress control,ϕ_i and ϕ_j keep on performing the stage-II ingress control to patterned whether they have some comparative indications. Accept that the individual health reports of patients ϕ_i and ϕ_j are $\overrightarrow{\beta} = (\beta_1, \beta_2, \ldots, \beta_n)$ and $\overrightarrow{\gamma} = (\gamma_1, \gamma_2, \ldots, \gamma_n)$, separately. ϕ_i first characterizes a threshold assessment th for the quantity of basic side effect characters. Keeping in mind the end goal to process $\overrightarrow{\beta} \cdot \overrightarrow{\gamma}$ in a privacy-preserving manner, ϕ_i and ϕ_j invoke the PPSPC scheme. For more details, related to PPSPC scheme, refer to Lu et al. (2013).

Meanwhile, the PPSPC scheme guarantees that neither ϕ_i nor ϕ_j will unveil their own healthcare records to each other amid the calculation of $\overrightarrow{\beta} \cdot \overrightarrow{\gamma}$ can effectively accomplish protection-preserving ingress control. For instance, if the given back value ends up being equivalent to or greater than the threshold assessment, to be specific $\overrightarrow{\beta} \cdot \overrightarrow{\gamma} \geq th$, at that point ϕ_j passes the stage-II ingress control and turns into a qualified partner. At that point, ϕ_i transfers the present session key $\kappa_i = h(\mathcal{T}^{\alpha}_{\jmath}(\mathcal{T}^{\alpha}_{\eta_i\vartheta_i}(\imath_1))(\bmod\, \varkappa)) \parallel \mathcal{PD})$ to ϕ_j. With the help of κ_i session key, ϕ_j can decrypt and develop the crude ρ_{hi} sent from ϕ_i's own BSN and after that transmit the handled ρ_{hi} to the healthcare center to minimize the liability on ϕ_i's SP. However, if the give-back value is smaller than the threshold assessment, to be specific $\overrightarrow{\beta} \cdot \overrightarrow{\gamma} < th$, at that point ϕ_j is not a qualified assistant to take an interest in the opportunistic computing process. If it is not too much trouble then, take note of that the threshold th is not settled. In case that the remaining energy of ϕ_i's SP is adequate, th can be fixed generally higher in order to limit the ρ_{hi} security exposure. In any case, if the remaining power is low, th ought to be fixed fairly in order to confirm the reliability of high-force ρ_{hi} preparation and communication tasks.

4 Examination of the proposed system

In this section, we will examine the efficiency of execution and security of our presented scheme and demonstrate that it can endure each possible attack. To start with, we will utilize the BAN logic in Lu et al. (2010b) to check the accuracy of presented scheme. At that point, we will show that no damage happens to the new scheme by the possible attacks. Finally, the execution efficiency will be examined for our scheme.

4.1 Security investigation and discussion

Here, we will investigate the security aspects of the planned scheme. We will not bring the man-in-the-middle attack here as it is dispensable on the estates that the opponent cannot conclude any isolated data noteworthy to the patient ϕ_i (or ϕ_j). Our new scheme has not just normally acquired every one of the qualities of its predecessor; it additionally settled the security flaws and holes.

Proposition 4.1 *The suggested system provides anonymity to the patient.*

Proof Based on the design of our proposed system, the excellent property of user anonymity can be guaranteed at

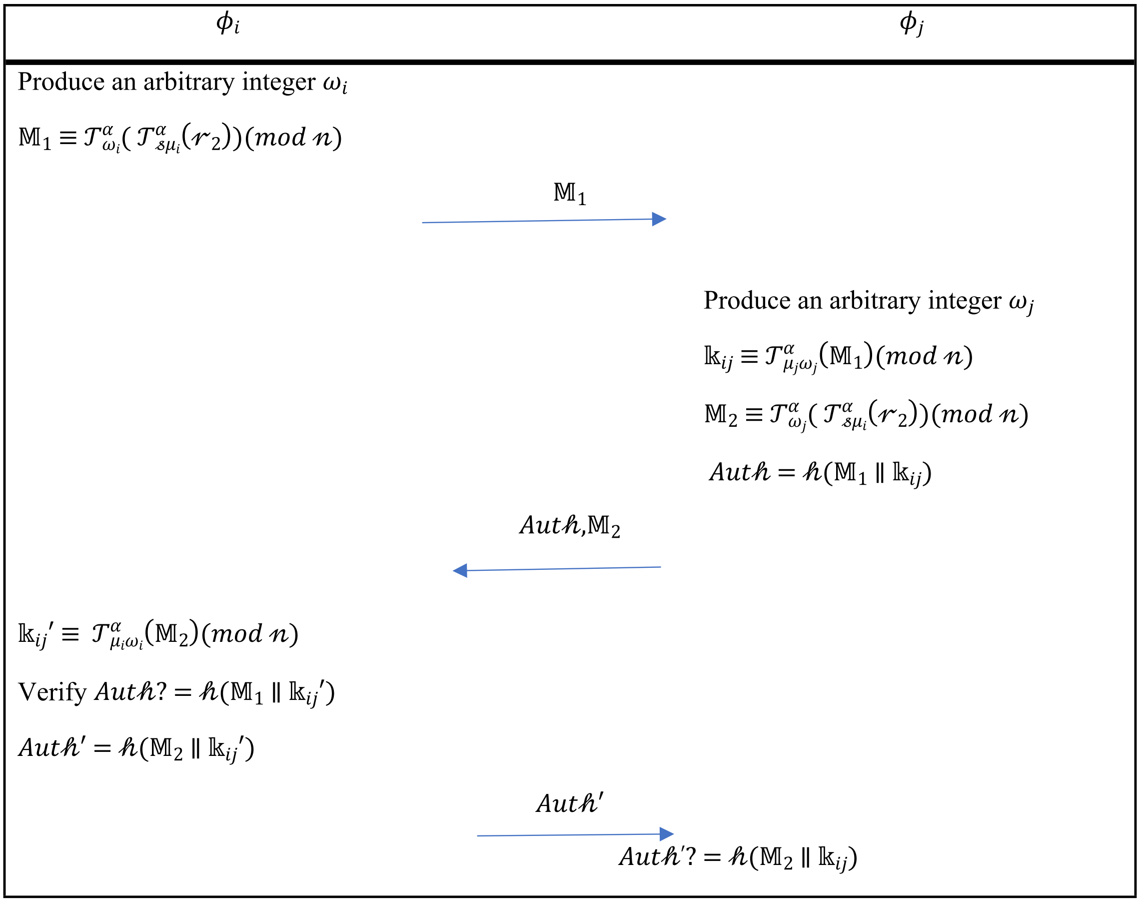

Fig. 5 Stage-I ingress control of propose system

every phase. An adversary may listen sneakily to the communication among the patient ϕ_i and the trusted center $\mathcal{TC}$, and attempt to follow the patient's genuine character to determine some security-delicate data of the patient. In the new scheme, the genuine character of the patient ϕ_i is ensured by $\boldsymbol{\kappa}_i = h(\mathcal{T}_{s}^{\alpha}(\mathcal{T}_{\eta_i\vartheta_i}^{\alpha}(r_1))(\text{mod}\ n)) \parallel \mathcal{PD})$. Keeping in mind that the end goal is to process $\mathcal{T}_{s}^{\alpha}(\mathcal{T}_{\eta_i\vartheta_i}^{\alpha}(r_1))(\text{mod}\ n)$, the foe will confront the conformable chaotic maps issue. Thus, our scheme can give the patient abnormal state anonymity.

Proposition 4.2 *The suggested system provides mutual authentication to the patient.*

Proof In the stage-I ingress control procedure of our new system, patient ϕ_i validates patient ϕ_j by examining the message $Auth? = h(\mathbb{M}_1 \parallel \mathbb{k}_{ij}')$ which ϕ_j sends to ϕ_i. Similarly, patient ϕ_j verifies patient ϕ_i by checking the message $Auth'? = h(\mathbb{M}_2 \parallel \mathbb{k}_{ij})$, *which* ϕ_i sent to ϕ_j. Now, $Auth'$ *and* $Auth$ both are incorporated into the common mutual session key $\mathbb{k}_{ij}$ among ϕ_i and ϕ_j. Along these lines, any adversary wishing to create messages will confront the conformable chaotic maps issue as well as the DHP. Therefore, the new scheme offers excellent mutual authentication among patients and is safe against the impersonation attack.

Proposition 4.3 *The presented system can resistance to replay attacks.*

Proof In our presented system, an adversary originally captures some correspondence data as per current key agreement system running in the replaying attack, and then returns the gathered data to the recipient running on future key agreement system. The proposed system break down fails by replaying attack in view of the reality that the freshness of text transmitted is supplied by the arbitrary nonce ω_i and ω_j. Aside from ϕ_i (or ϕ_j), just ϕ_j (or ϕ_i) can connect the communal mutual meeting key $\mathbb{k}_{ij}$ and the message with arbitrary nonce $Auth$ (or $Auth'$), individually. Henceforth, the suggested system is safe against replaying attack.

Proposition 4.4 *The suggested system can tolerate the Bergamo et al.'s attack.*

Proof The attack by Bergamo et al. (2005) is based on the condition that an adversary may obtain the related elements r_2, $\mathcal{T}_{\omega_i}^{\alpha}(\mathcal{T}_{s\mu_i}^{\alpha}(r_2))(\text{mod}\ n)$, $\mathcal{T}_{\omega_j}^{\alpha}(\mathcal{T}_{s\mu_j}^{\alpha}(r_2))(\text{mod}\ n)$,

$\mathcal{T}^{\alpha}_{\jmath\mu_j}(\imath_2)(\bmod\,\varkappa)$ and $\mathcal{T}^{\alpha}_{\jmath\mu_j}(\imath_2))(\bmod\,\varkappa)$. In our system, the adversary could easily get $\mathcal{T}^{\alpha}_{\omega_i}(\mathcal{T}^{\alpha}_{\jmath\mu_i}(\imath_2))(\bmod\,\varkappa)$ and $\mathcal{T}^{\alpha}_{\omega_j}\left(\mathcal{T}^{\alpha}_{\jmath\mu_j}(\imath_2)\right)(\bmod\,\varkappa)$, but there is no way to get $\imath_2$, $\mathcal{T}^{\alpha}_{\jmath\mu_i}(\imath_2)(\bmod\,\varkappa)$ and $\mathcal{T}^{\alpha}_{\jmath\mu_j}(\imath_2)(\bmod\,\varkappa)$, even though the opponent is a legitimate medical patient. The aim for this is that the essentials diffused through a safe channel and are known only to the medical user/patient and the trusted authority. In addition, our new system uses the conformable Chebyshev polynomials, where the periodicity of the cosine function is escaped by extending the interval of $\imath_2$ to $(-\infty, +\infty)$. Therefore, the attack by Bergamo et al. would have no effect on cracking our proposed system.

4.2 Formal Authentication proof of propose scheme using BAN Logic

In order to analyze data trade schemes, we adopted the standard approaches i.e., BAN-logic. To utilize the BAN logic, we should characterize the essential notations, objectives, and suspicions first. At that point, we shall check the accurateness of the novel scheme as explained below.

4.2.1 Notations

We will primarily explore the BAN logic's sentence structure. We characterize $\mathfrak{F}$ and $\mathfrak{B}$ as participators, $\sqcap$ as an equation, and certain instances are utilized to look at the BAN logic's language structure and notations (Lu et al. 2010b,2012).

- $\mathfrak{F}|\equiv\imath_1$: $\mathfrak{F}$ trusts $\imath_1$ is an exact.
- $\mathfrak{F}\triangleleft\imath_1$: $\mathfrak{F}$ sees or holds $\imath_1$.
- $\mathfrak{F}|\equiv\mathfrak{B}$: $\mathfrak{F}$ trusts $\mathfrak{B}$'s activities; e.g., $\mathfrak{F}|\equiv\mathfrak{B}\triangleleft\imath_1$ implies that $\mathfrak{F}$ trusts that $\mathfrak{B}$ holds $\imath_1$.
- $\mathfrak{F}|\Rightarrow\imath_1$: $\mathfrak{F}$ has full $\imath_1$ control. This can be used to signify an agency for certificates.
- $\mathfrak{F}|\sim\imath_1$: $\mathfrak{F}$ once communicated message $\imath_1$.
- $\#(\imath_1)$: $\imath_1$ is crisp; that implies $\imath_1$ is later or nonce, $\imath_1$.
- $\mathfrak{F}\overset{r_1}{\leftrightarrow}\mathfrak{B}$: a secret info, $\imath_1$ or secret key shared among $\mathfrak{F}$ and $\mathfrak{B}$.
- $\overset{\imath_1}{\mapsto}\mathfrak{F}$ and $\imath_1^{-1}$: $\mathfrak{F}$ has $\imath_1$ and $\imath_1^{-1}$, as public key and secret key, respectively.
- $\{\mathbb{M}\}_{\imath_1}$: $\imath_1$ encrypts plain text M.
- $(\imath_1, \imath_2)$: $\imath_1$ or $\imath_2$ is one part of formulation $(\imath_1, \imath_2)$.
- $\frac{\text{Rule1}}{\text{Rule2}}$: Rule 2 of Rule 1 may be construed; e.g., $\frac{\mathfrak{F}\text{createsrandom}\imath_1}{\mathfrak{F}|\equiv(\imath_1)}$ implies that $\mathfrak{F}$ makes $\imath_1$, so $\mathfrak{F}$ trusts $\imath_1$ is new.

Using the BAN logic, we deciphered an idealized shape of a new system (as described in Fig. 5):

M1 $\phi_i \rightarrow \phi_j : \{\imath_2\}_{(\Bbbk_{\mathcal{TC}}^{-1}\cdot\mathcal{TC}\overset{\mu_i}{\leftrightarrow}\phi_i\cdot\omega_i)}$

M2 $\phi_j \rightarrow \phi_i : \hslash(\{\imath_2\}_{(\Bbbk_{\mathcal{TC}}^{-1}\cdot\mathcal{TC}\overset{\mu_i}{\leftrightarrow}\phi_i\cdot\omega_i)},$
$\phi_i\overset{\Bbbk_{ij}}{\leftrightarrow}\phi_j), \{\imath_2\}_{(\Bbbk_{\mathcal{TC}}^{-1}\cdot\mathcal{TC}\overset{\mu_j}{\leftrightarrow}\phi_j\cdot\omega_j)}$

M3 $\phi_i \rightarrow \phi_j : \hslash(\{\imath_2\}_{(\Bbbk_{\mathcal{TC}}^{-1}\cdot\mathcal{TC}\overset{\mu_j}{\leftrightarrow}\phi_j\cdot\omega_j)}, \phi_i\overset{\Bbbk_{ij}}{\leftrightarrow}\phi_j)$

4.2.2 Objectives

We will analyze the objectives of proposed scheme here. In the proposed scheme, patient ϕ_i, patient ϕ_j, and $\mathcal{TC}$ are the contenders. The stage-I ingress control of new scheme has the accompanying two objectives: (a) ϕ_i trusts ϕ_j; an authorized patient, and (b) ϕ_j trusts ϕ_i; an authorized patient. The objectives of new scheme are shown as equations 1 and 2 in the dialect of the BAN logic.

$\mathcal{O}1.$ $\phi_i|\equiv\phi_j\triangleleft\{\imath_2\}_{(\Bbbk_{\mathcal{TC}}^{-1})}$

$\mathcal{O}2.$ $\phi_j|\equiv\phi_i\triangleleft\{\imath_2\}_{(\Bbbk_{\mathcal{TC}}^{-1})}$

4.2.3 Expectations

Now, we slope some connected outlooks:

ε1. $\phi_i|\equiv\#(\omega_i)$

ε2. $\phi_j|\equiv\#(\omega_j)$

ε3. $\phi_i|\equiv\overset{\Bbbk}{\mapsto}\mathcal{TC}$

ε4. $\phi_j|\equiv\overset{\Bbbk}{\mapsto}\mathcal{TC}$

ε5. $\phi_i|\equiv\mathcal{TC}|\Rightarrow\{\imath_2\}_{(\Bbbk_{\mathcal{TC}}^{-1},\mathcal{TC}\overset{\mu_i}{\leftrightarrow}\phi_i)}$

ε6. $\phi_j|\equiv\mathcal{TC}|\Rightarrow\{\imath_2\}_{(\Bbbk_{\mathcal{TC}}^{-1},\mathcal{TC}\overset{\mu_j}{\leftrightarrow}\phi_j)}$

ε7. $\phi_i|\equiv\mathcal{TC}\overset{\mu_i}{\leftrightarrow}\phi_i$

ε8. $\phi_j|\equiv\mathcal{TC}\overset{\mu_j}{\leftrightarrow}\phi_j$

ε9. $\mathcal{TC}|\Rightarrow\{\imath_2\}_{(\Bbbk_{\mathcal{TC}}^{-1})}$

4.2.4 Verification

The principle ventures of the evidence are as shown below.

ϕ_i picks an arbitrary value ω_i

V1. $\phi_i|\equiv\omega_i$

V2. $\phi_i|\equiv\#(\omega_i)$

Message 1: $\phi_i \rightarrow \phi_j$: $\{\imath_2\}_{(\Bbbk_{\mathcal{TC}}^{-1},\mathcal{TC}\overset{\mu_i}{\leftrightarrow}\phi_i,\omega_i)}$

V3. $\phi_j\triangleleft\{\imath_2\}_{(\Bbbk_{\mathcal{TC}}^{-1},\mathcal{TC}\overset{\mu_i}{\leftrightarrow}\phi_i,\omega_i)}$

ϕ_j picks arbitrary ω_j

V4. $\phi_j|\equiv\omega_j$

V5. $\phi_j|\equiv\#(\omega_j)$

ϕ_j calculates

$$\phi_i\overset{\Bbbk_{ij}}{\leftrightarrow}\phi_j = \left\{\{\imath_2\}_{(\Bbbk_{\mathcal{TC}}^{-1},\mathcal{TC}\overset{\mu_i}{\leftrightarrow}\phi_i,\omega_i)}\right\}_{(\mathcal{TC}\overset{\mu_j}{\leftrightarrow}\phi_j,\omega_j)}$$
$$= \{\imath_2\}_{(\Bbbk_{\mathcal{TC}}^{-1},\mathcal{TC}\overset{\mu_i}{\leftrightarrow}\phi_i,\omega_i,\mathcal{TC}\overset{\mu_j}{\leftrightarrow}\phi_j,\omega_j)}$$

Message 2: $\phi_j \rightarrow \phi_i$: $\mathscr{h}(\{\mathscr{r}_2\}_{(\Bbbk_{\mathcal{TC}}^{-1}, \mathcal{TC} \overset{\mu_i}{\longleftrightarrow} \phi_i, \omega_i)}, \phi_i \overset{\Bbbk_{ij}}{\longleftrightarrow} \phi_j)$, $\{\mathscr{r}_2\}_{(\Bbbk_{\mathcal{TC}}^{-1}, \mathcal{TC} \overset{\mu_j}{\longleftrightarrow} \phi_j, \omega_j)}$

V6. $\phi_i \lhd \mathscr{h}(\{\mathscr{r}_2\}_{(\Bbbk_{\mathcal{TC}}^{-1}, \mathcal{TC} \overset{\mu_i}{\longleftrightarrow} \phi_i, \omega_i)}, \phi_i \overset{\Bbbk_{ij}}{\longleftrightarrow} \phi_j), \{\mathscr{r}_2\}_{(\Bbbk_{\mathcal{TC}}^{-1}, \mathcal{TC} \overset{\mu_j}{\longleftrightarrow} \phi_j, \omega_j)}$

V7. $$\frac{\phi_i \lhd \omega_i, \phi_i \lhd \mathcal{TC} \overset{\mu_i}{\longleftrightarrow} \phi_i, \phi_i \lhd \{r_1\}_{(\Bbbk_{\mathcal{TC}}^{-1}, \mathcal{TC} \overset{\mu_j}{\longleftrightarrow} \phi_j, \omega_j)}}{\phi_i \lhd \phi_i \overset{\Bbbk_{ij}}{\longleftrightarrow} \phi_j}$$

V8. $$\frac{\phi_i \lhd \mathscr{h}\left(\{\mathscr{r}_2\}_{(\Bbbk_{\mathcal{TC}}^{-1}, \mathcal{TC} \overset{\mu_i}{\longleftrightarrow} \phi_i, \omega_i)}, \phi_i \overset{\Bbbk_{ij}}{\longleftrightarrow} \phi_j\right), \phi_i \lhd \phi_i \overset{\Bbbk_{ij}}{\longleftrightarrow} \phi_j, \phi_i| \equiv \{\mathscr{r}_2\}_{(\Bbbk_{\mathcal{TC}}^{-1}, \mathcal{TC} \overset{\mu_i}{\longleftrightarrow} \phi_i)}, \phi_i| \equiv \omega_i}{\phi_i| \equiv \phi_i \overset{\Bbbk_{ij}}{\longleftrightarrow} \phi_j}$$

V9. $$\frac{\phi_i| \equiv \phi_i \overset{\Bbbk_{ij}}{\longleftrightarrow} \phi_j}{\phi_i| \equiv \phi_j| \sim \{\mathscr{r}_2\}_{\left(\Bbbk_{\mathcal{TC}}^{-1}, \mathcal{TC} \overset{\mu_j}{\longleftrightarrow} \phi_j, \omega_j\right)}}$$

V10. $$\frac{\phi_i| \equiv \phi_j| \sim \{\mathscr{r}_2\}_{\left(\Bbbk_{\mathcal{TC}}^{-1}, \mathcal{TC} \overset{\mu_j}{\longleftrightarrow} \phi_j, \omega_j\right)}, \phi_i| \equiv \phi_i \overset{\Bbbk_{ij}}{\longleftrightarrow} \phi_j, \phi_i| \equiv \overset{\Bbbk}{\mapsto} \mathcal{TC}, \phi_i| \equiv \#(\omega_i)}{\phi_i| \equiv \phi_j \lhd \{r_1\}_{(\Bbbk_{\mathcal{TC}}^{-1})}}$$

Message 3: $\phi_i \rightarrow \phi_j$: $\mathscr{h}(\{\mathscr{r}_2\}_{\left(\Bbbk_{\mathcal{TC}}^{-1}, \mathcal{TC} \overset{\mu_j}{\longleftrightarrow} \phi_j, \omega_j\right)}, \phi_i \overset{\Bbbk_{ij}}{\longleftrightarrow} \phi_j)$

V11. $\phi_j \lhd \mathscr{h}(\{\mathscr{r}_2\}_{\left(\Bbbk_{\mathcal{TC}}^{-1}, \mathcal{TC} \overset{\mu_j}{\longleftrightarrow} \phi_j, \omega_j\right)}, \phi_i \overset{\Bbbk_{ij}}{\longleftrightarrow} \phi_j)$

V12. $$\frac{\phi_j \lhd \mathscr{h}\left(\{\mathscr{r}_2\}_{\left(\Bbbk_{\mathcal{TC}}^{-1}, \mathcal{TC} \overset{\mu_j}{\longleftrightarrow} \phi_j, \omega_j\right)}, \phi_i \overset{\Bbbk_{ij}}{\longleftrightarrow} \phi_j\right), \phi_j \lhd \phi_i \overset{\Bbbk_{ij}}{\longleftrightarrow} \phi_j,}{\phi_j| \equiv \phi_i \lhd \phi_i \overset{\Bbbk_{ij}}{\longleftrightarrow} \phi_j}$$

V13. $$\frac{\phi_j| \equiv \phi_i \lhd \phi_i \overset{\Bbbk_{ij}}{\longleftrightarrow} \phi_j}{\phi_j| \equiv \phi_i \lhd \{r_2\}_{(\Bbbk_{\mathcal{TC}}^{-1})}}$$

Subsequently, deriving from equations V1 and V10, we can now be assured that a new scheme is really equipped to accomplish the objectives.

4.3 Performance investigation

In this segment, we will measure the execution time of the proposed scheme. To do so, the experimentations are conducted on Intel Core i5-8365U CPU @1.90 GHz with 8 GB RAM and 1 TB HDD using 64-bit Windows 10 operating system. Moreover, to check authenticity and security properties, we adopted Automated Validation of Internet Security Protocols and Applications (AVISPA) (http://www.avispa-project.org/). In addition, High-Level

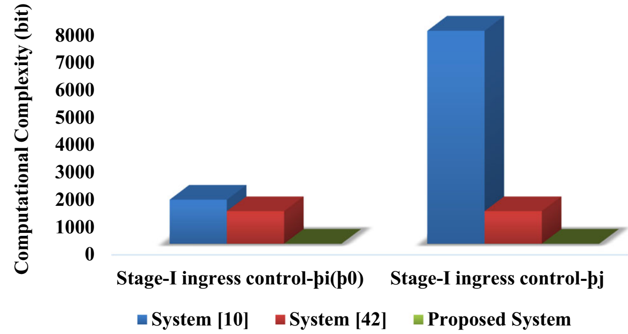

Fig. 6 Computational complexity (bit)

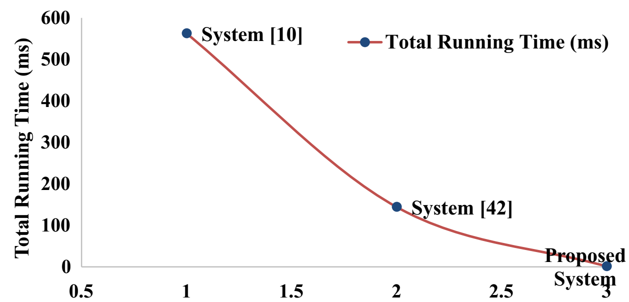

Fig. 7 Total running time (ms)

Protocol Specification Language (HLPSL) is utilized to model the verification of new system using AVISPA v.1.1.

The assessment of the security properties between Lu et al. (2013) and Meshram et al. (2020) and our proposed system is demonstrated in Table 2. The latter also shows the evaluation of the computational complexity of the stage-I ingress control in the suggested system and total running time (ms) in Figs. 6 and 7, and that of systems in Lu et al. (2013) and Meshram et al. (2020). Let $\mathcal{T}_{hash}, \mathcal{T}_{exp}, \mathcal{T}_{pair}, \mathcal{T}_{chaotic}$ and $\mathcal{T}_{ecsm}$ denote the execution time for a one-way hash function, one modular exponentiation in group, one pairing operation, chaotic map operation and one-point scale multiplication over elliptic curve,

Table 1 Symbols utilized in the organized scheme

Symbol	Definition
ϕ_i, ϕ_j	The medical patient
$\mathcal{TC}$	A trusted center
$\mathscr{n}$	Large integer $\mathscr{n} = \mathscr{q}\mathscr{p}$, where $\mathscr{q}$ and $\mathscr{p}$ be large primes with $\mathscr{p}\|(\mathscr{q} - 1)$
$\mathscr{s}$	Random integer as master key, picked by the trusted center
$\mathcal{T}$	Conformable chaotic maps operator
$\mathscr{r}_1, \mathscr{r}_2$	Two random numbers picked by the trusted center
ϑ_i, μ_i	Two random integers picked by the trusted center for patient ϕ_i
$\eta_i, \omega_i, \omega_j$	Three random integers
$\mathscr{h}(\bullet)$	A endangered hash function
$\|\|$	The concatenation operation $\mathscr{h}$

Table 2 Assessment of the computational complexity and security properties

Systems /computational complexity and security properties	Lu et al. (2013)	Meshram et al. (2020)	Proposed system
Stage-I ingress control-$\phi_i(\phi_0)$	$\mathcal{T}_{pair} + \mathcal{T}_{ecsm} = 1622.5\mathcal{T}_{hash}$	$2(\mathcal{T}_{exp} + \mathcal{T}_{hash}) = 1202\mathcal{T}_{hash}$	$2(\mathcal{T}_{chaotic} + \mathcal{T}_{hash}) = 4\mathcal{T}_{hash}$
Stage-I ingress control-ϕ_j	$5\mathcal{T}_{pair} = 7750\mathcal{T}_{hash}$	$2(\mathcal{T}_{exp} + \mathcal{T}_{hash}) = 1202\mathcal{T}_{hash}$	$2(\mathcal{T}_{chaotic} + \mathcal{T}_{hash}) = 4\mathcal{T}_{hash}$
Replay attack	N	Y	Y
Patient anonymity	N	Y	Y
Mutual authentication	N	Y	Y
Bergamo et al. attack	N	N	Y

Y The scheme can resist the risk and N the scheme cannot resist the risk

respectively. From Table 2, Figs. 6 and 7, and by using the experimental results obtained in Burrows et al. (1989), Wessels (2001), Liu et al. (2014), Guelzim et al. (2016), Zhao (2014), Cao and Kou (2010), Lee et al. (2013), Verma et al. (2020), Ibrahim et al. (2016), the accompanying computation time is mapped as the time unit for the hashing time: $\mathcal{T}_{exp} = 600\mathcal{T}_{hash}$, $\mathcal{T}_{hash} \approx \mathcal{T}_{chaotic}$, $\mathcal{T}_{ecsm} = 72.5\mathcal{T}_{hash}$, and $\mathcal{T}_{pair} = 1550\mathcal{T}_{hash}$. Therefore, we have the associated connection in terms of computational complexity:$\mathcal{T}_{hash} \approx \mathcal{T}_{chaotic} < \mathcal{T}_{exp} < \mathcal{T}_{ecsm} < \mathcal{T}_{exp} < \mathcal{T}_{pair}$. The processing time for $\mathcal{T}_{hash}$ is 0.06 ms (Guelzim et al. 2016). Bilinear pairings to execute the stage-I ingress control are utilized in Lu et al. (2013) and Meshram et al. (2020), and subsequently computational complexity nature of their scheme is $\mathcal{T}_{ecsm} + 6\mathcal{T}_{pair}$ and$4\mathcal{T}_{hash} + 4\mathcal{T}_{exp}$, which are equal to 562.35 ms and 144.24 ms, respectively. By differentiating, computational complexity of our proposed system is $4\mathcal{T}_{hash} + 4\mathcal{T}_{chaotic}$, which is equal to only 1.22 ms. Here we choose $\alpha = 1/2$, since $\alpha\epsilon[0, 1]$ by Definition 2.1 (Sect. 2). The main advantage of the new scheme's execution when compared to these in Lu et al. (2013) and Meshram et al. (2020) is systems originate from our selection of the conformable chaotic maps operation rather than bilinear pairings and partial discrete logarithm.

5 Conclusion

In this paper, we proposed a new efficient *m*-healthcare emerging emergency medical system using conformable chaotic maps. The proposed authentication system can accept auxiliary patient anonymity. Additionally, we performed mutual authentication with a specific ultimate goal to determine those security problems while providing better computing effectiveness. Clearly, the presented system is more secure and more practical than other the systems available in the literature as mentioned above. Furthermore, our proposed system can balance the high-intensive PHI communication and transmission and minimize the disclosure of PHI privacy in m-Healthcare emerging emergency.

Acknowledgements The authors are grateful to the learned reviewers and their critical comments. Their comments have guided the authors to improve the manuscript.

Declarations

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

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

Informed consent N/A.

References

Abd El-Latif AA, Abd-El-Atty B, Abou-Nassar EM, Venegas-Andraca SE (2020a) Controlled alternate quantum walks based privacy preserving healthcare images in internet of things. Optics Laser Technol 124:105942

Abd El-Latif AA, Abd-El-Atty B, Mazurczyk W, Fung C, Venegas-Andraca SE (2020b) Secure data encryption based on quantum walks for 5G Internet of Things scenario. IEEE Trans Netw Serv Manag 17(1):118–131

Abd El-Latif AA, Abd-El-Atty B, Venegas-Andraca SE, Elwahsh H, Piran MJ, Bashir AK et al (2020c) Providing end-to-end security using quantum walks in IoT networks. IEEE Access

Abd-El-Atty B, Iliyasu AM, Alaskar H, El-Latif A, Ahmed A (2020) A robust quasi-quantum walks-based steganography protocol for secure transmission of images on cloud-based E-healthcare platforms. Sensors 20(11):3108

Abou-Nassar EM, Iliyasu AM, El-Kafrawy PM, Song OY, Bashir AK, Abd El-Latif AA (2020) DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems. IEEE Access 8:111223–111238

Alghamdi A, Hammad M, Ugail H (2020) Detection of myocardial infarction based on novel deep transfer learning methods for urban healthcare in smart cities. Multimed Tools Appl. https://doi.org/10.1007/s11042-020-08769-x

Amirbekyan A, Estivill-Castro V (2007) A new efficient privacy-preserving scalar product protocol. In: Proceedings of AusDM'07, pp 209–214

Anderson DR, Camrud E, Ulness DJ (2018) On the nature of the conformable derivative and its applications to physics. arXiv preprint arXiv:1810.02005

Bergamo P, D'Arco P, Santis A, Kocarev L (2005) Security of public key cryptosystems based on Chebyshev polynomials. IEEE Trans Circuits Syst I 52(7):1382–1393

Boneh D, Franklin MK (2001) Identity-based encryption from the weil pairing. In: Proceedings of CRYPTO'01, pp 213–229

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

Cao X, Kou W (2010) A pairing-free identity-based authenticated key agreement scheme with minimal message exchanges. Inf Sci 180:2895–2903

Chen F, Liao X, Wong KW, Han Q, Li Y (2012) Period distribution analysis of some linear maps. Commun Nonlinear Sci Numer Simul 17:3848–3856

Conti M, Kumar M (2010) Opportunities in opportunistic computing. IEEE Comput 43(1):42–50

Conti M, Giordano S, May M, Passarella A (2010) From opportunistic networks to opportunistic computing. IEEE Commun Mag 48(9):126–139

Dhurandher SK, Kumar A, Obaidat MS (2018) Cryptography-based misbehavior detection and trust control mechanism for opportunistic network systems. IEEE Syst J 12(4):3191–3202

Du W, Atallah M (2001) Privacy-preserving cooperative statistical analysis. In: Proceedings of ACSAC'01, pp 102–111

El-Latif AAA, Hossain MS, Wang N (2019) Score level multibiometrics fusion approach for healthcare. Clust Comput 22:2425–2436. https://doi.org/10.1007/s10586-017-1287-4

Elliot M, Purdam K, Smith D (2008) Statistical disclosure control architectures for patient records in biomedical information systems. J Biomed Inform 41:58–64

Employee Benefit Research Institute, Retirement Confidence Survey [Online]. Available: http://www.ebri.org/surveys/hcs/ (2008)

Guelzim T, Obaidat MS, Sadoun B (2016) Introduction and overview of key enabling technologies for smart cities and homes. In: Smart cities and homes: key enabling technologies, pp 1–16

Han S, Chang E (2009) Chaotic map based key agreement with/out clock synchronization. Choas Soliton Fractals 39(3):1283–1289

Ibrahim MH, Kumari S, Das AK, Wazid M, Odelu V (2016) Secure anonymous mutual authentication for star two-tier wireless body area networks. Comput Methods Programs Biomed 135:37–50

Klasnja P, Pratt W (2012) Healthcare in the pocket: mapping the space of mobile-phone health interventions. J Biomed Inform 45:184–198

Lee CC, Hsu CW, Lai YM, Vasilakos A (2013) An enhanced mobile-healthcare emergency system based on extended chaotic maps. J Med Syst 37:9973

Li M, Lou W, Ren K (2010) Data security and privacy in wireless body area networks. IEEE Wirel Commun 17(1):51–58

Li M, Yu S, Zheng Y, Ren K, Lou W (2013) Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Trans Parallel Distrib Syst 24(1):131–143

Lin X, Sun X, Ho P, Shen X (2007) Gsis: a secure and privacy preserving protocol for vehicular communications. IEEE Trans Veh Technol 56(6):3442–3456

Lin X, Lu R, Shen X, Nemoto Y, Kato N (2009) Sage: a strong privacy-preserving scheme against global eavesdropping for ehealth systems. IEEE J Sel Areas Commun 27(4):365–378

Liu JW, Zhang ZH, Chen XF, Kwak KS (2014) Certificateless remote anonymous authentication schemes for wireless body area networks. IEEE Trans Parallel Distrib Syst 25(2):332–342

Lu H, Lane ND, Eisenman SB, Campbell AT (2010a) Bubble-sensing: binding sensing tasks to the physical world. Ubiquitous Mob Comput 6(1):58–71

Lu R, Lin X, Zhu H, Shen X (2010b) An intelligent secure and privacy-preserving parking scheme through vehicular communications. IEEE Trans Veh Technol 59(6):2772–2785

Lu R, Lin X, Liang X, Shen X (2011) A secure handshake scheme with symptoms-matching for m-healthcare social network. Mob Netw Appl 16(6):683–694

Lu R, Lin X, Luan H, Liang X, Shen X (2012) Pseudonym changing at social spots: an effective strategy for location privacy in VANETs. IEEE Trans Veh Technol 61(1):86–96

Lu R, Lin X, Shen X (2013) SPOC: a secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency. IEEE Trans Parallel Distrib Syst 24(3):614–624

Malin B, Sweeney L (2004) How (not) to protect genomic data privacy in a distributed network: using trail re-identification to evaluate and design anonymity protection systems. J Biomed Inform 37:179–192

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

Mason JC, Handscomb DC (2003) Chebyshev polynomials. Chapman & Hall/CRC, Boca Raton

Meshram C, Meshram SA, Zhang M (2012) An ID-based cryptographic mechanisms based on GDLP and IFP. Inf Process Lett 112(19):753–758

Meshram C, Lee CC, Li CT, Chen CL (2017a) A secure key authentication scheme for cryptosystems based on GDLP and IFP. Soft Comput 21(24):7285–7291

Meshram C, Tseng YM, Lee CC, Meshram SG (2017b) An IND-ID-CPA secure ID-based cryptographic protocol using GDLP and IFP. Informatica 28(3):471–484

Meshram C, Li CT, Meshram SG (2019a) An efficient online/offline id-based short signature procedure using extended chaotic maps. Soft Comput 23(3):747–753

Meshram C, Lee CC, Meshram SG, Li CT (2019b) An efficient ID-based cryptographic transformation model for extended chaotic-map-based cryptosystem. Soft Comput 23(16):6937–6946

Meshram C, Lee CC, Meshram SG, Ramteke RJ, Meshram A (2020) An efficient mobile-healthcare emergency framework. J Med Syst 44(58):1–14

[Online]. Available: http://www.research2guidance.com/us-1.3-billion-the-market-for-mhealth-applications-in-2012/

Rault T, Bouabdallah A, Challal Y, Marin F (2017) A survey of energy-efficient context recognition systems using wearable sensors for healthcare applications. Ubiquitous Mob Comput 37:23–44

Ren Y, Pazzi RWN, Boukerche A (2010) Monitoring patients via a secure and mobile healthcare system. IEEE Wirel Commun 17(1):59–65

Roy A, Mondal A, Misra S, Obaidat MS (2020) ORCID: opportunistic reconnectivity for network management in the presence of dumb nodes in wireless sensor networks. IEEE Syst J 14(1):9–16

Silva Bruno MC, Rodrigues Joel JPC, de la Torre DI, López-Coronado M, Saleem K (2015) Mobile-health: a review of current state in 2015. J Biomed Inform 56:265–272

Sun J, Fang Y (2010) Cross-domain data sharing in distributed electronic health record systems. IEEE Trans Parallel Distrib Syst 21(6):754–764

The AVISPA Project, funded by the European Union in the Future and Emerging Technologies (FET Open) programme, Project Number: IST-2001–39252, 2003. http://www.avispa-project.org/

Toninelli A, Montanari R, Corradi A (2009) Enabling secure service discovery in mobile healthcare enterprise networks. IEEE Wirel Commun 16(3):24–32

Tsafack N, Kengne J, Abd-El-Atty B, Iliyasu AM, Hirota K, Abd El-Latif AA (2020) Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption. Inf Sci 515:191–217
Tsafack N, Sankar S, Abd-El-Atty B, Kengne J, Jithin KC, Belazi A, Abd El-Latif AA (2020a) A new chaotic map with dynamic analysis and encryption application in internet of health things. IEEE Access 8:137731–137744
Vaidya J, Clifton C (2002) Privacy preserving association rule mining in vertically partitioned data. In: Proceedings of ACM KDD'02, pp 639–644
Verma GK, Singh BB, Kumar N, Obaidat MS, He D, Singh H (2020) An Efficient and provable certificate-based proxy signature scheme for IIoT environment. Inf Sci 518:142–156
Wessels J (2001) Application of BAN-Logic. CMG Public Sector B.V., 2001. http://www.win.tue.nl/ipa/archive/springdays2001/banwessels.pdf. Accessed 20 Dec 2012
Yuce MR, Ng SWP, Myo NL, Khan JY, Liu W (2007) Wireless body sensor network using medical implant band. J Med Syst 31(6):467–474
Zhang L (2008) Cryptanalysis of the public key encryption based on multiple chaotic systems. Chaos Solitons Fractals 37(3):669–674
Zhao Z (2014) An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem. J Med Syst 38(2):1–7
Zhou J, Cao Z, Dong X, Lin X, Vasilakos AV (2013) Securing m-healthcare social networks: challenges, countermeasures and future directions. IEEE Wirel Commun 20(4):12–21

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