Multimedia Tools and Applications (2021) 80:17103–17128
https://doi.org/10.1007/s11042-020-10134-x

1157T: INTELLIGENT MULTIMEDIA NETWORKS

Chaotic-map based authenticated security framework with privacy preservation for remote point-of-care

B. D. Deebak, et al. *[full author details at the end of the article]*

Received: 17 December 2019 / Revised: 13 October 2020 / Accepted: 23 October 2020 /
Published online: 12 November 2020

Abstract
The challenge of COVID-19 has become more prevalent across the world. It is highly demanding an intelligent strategy to outline the precaution measures until the clinical trials find a successful vaccine. With technological advancement, Wireless Multimedia Sensor Networks (WMSNs) has extended its significant role in the development of remote medical point-of-care (RM-PoC). WMSN is generally located on a communication device to sense the vital signaling information that may periodically be transmitted to remote intelligent pouch This modern remote system finds a suitable professional system to inspect the environment condition remotely in order to facilitate the intelligent process. In the past, the RM-PoC has gained more attention for the exploitation of real-time monitoring, treatment follow-up, and action report generation. Even though it has additional advantages in comparison with conventional systems, issues such as security and privacy are seriously considered to protect the modern system information over insecure public networks. Therefore, this study presents a novel Single User Sign-In (SUSI) Mechanism that makes certain of privacy preservation to ensure better protection of multimedia data. It can be achieved over the negotiation of a shared session-key to perform encryption or decryption of sensitive data during the authentication phase. To comply with key agreement properties such as appropriate mutual authentication and secure session key-agreement, a proposed system design is incorporated into the chaotic-map. The above assumption claims that it can not only achieve better security efficiencies but also can moderate the computation, communication, and storage cost of some intelligent systems as compared to elliptic-curve cryptography or RSA. Importantly, in order to offer untraceability and user anonymity, the RM-PoC acquires dynamic identities from proposed SUSI. Moreover, the security efficiencies of proposed SUSI are demonstrated using informal and formal analysis of the real-or-random (RoR) model. Lastly, a simulation study using NS3 is extensively conducted to analyze the communication metrics such as transmission delay, throughput rate, and packet delivery ratio that demonstrates the significance of the proposed SUSI scheme.

Keywords Remote point-of-care · Authentication · And key agreement · Security and privacy · Chaotic-map · Real-or-random

1 Introduction

The spread of novel coronavirus known as COVID-19 has escalated drastically across the globe as a pandemic in early March 2020. It has become an outbreak of a global health emergency that searches a new technology to tackle the pandemic situation of the COVID-19. Of the information age, the digital applications have highly been recommended for the coordination effects of government and people. It includes early surveillance to perform effective contact tracing, testing, and strict quarantine. Most of the countries integrate the policies and healthcare in the digital technologies to facilitate pandemic planning including government coordination, treatments, hospital infrastructures, clinical management, medical supplies, screening, and containment zones. It uses big data and artificial intelligence as the effective tools to monitor and control the infection and mortality rate. To track the movement of the common people, a tool known as a migration map is utilized. It has been enabled in the smartphone, payment applications, and social media to infer the people location. It may periodically collect the data movements of the people to forecast the regional transmissions. It can also be more useful to guide the border checkup and surveillance. In addition, few countries have developed a dedicated application such as Aarogya Setu, Stopp Corona, COVIDSafe, Alipay, and smittestop that reports the data volume of active and discharge COVID-19 patients, staffing, protection equipment, and other information resources.

1.1 Implication of PoC

PoC is widely used as a diagnostic device to acquire the medical data of the patient. It has limited-resource settings to offer a clinical procedure that demands high-end instruments to perform results interpretation surgical clearance, and medical diagnosis. Since it demands a lot of improvements to meet the objectives of the healthcare systems, the practical use is still at the beginning phase. The PoC testing is still effective to obtain the clinical information that quickly performs the test procurement to treat the patients at the earliest. It may ultimately reduce turn-around time between the registration process to the report generation. Most of the developed countries apply the PoC test that changes the diagnostic process ranging from intensive care to personal care. However, the medical facilities draw the attention to the complex scenario to accommodate the diverse population across the globe. Despite the global advancements in diagnostic technologies, developing countries such as India, Thailand, and UAE face a major issue of automation. In the past, a remote point-of-care (PoC) has attracted research attention for its simplicity and convenience. In contrast to the conventional medical system, the PoC has several benefits such as assistive technology to the senior people, superior tractability for private healthcare bid organization providing maximum resource utilization [34].

In general, the PoC applications are associated with a series of interconnectivity devices, namely medical sensors, smartphones, and smart home-based gateway. The implantable curative sensors are positioned on the victim's body to read and gather the functional data comprising heart bit-rate, temperature, sugar-value, etc. The sensing information is collected through a smartphone and transmitted to a remote server or terminal through the wireless gateway. Through the act of PoC healthcare applications, remote monitoring is having the abilities of several high-quality services such as emergency service and medical treatment. The PoC application may provide a novel approach for the diagnosis of rare medical treatment and the patient's summary report generation. Due to its inherent capacity, the PoC has gained more

application benefits for commercial enterprises. Since the biological data is extremely sensitive, privacy preservation is becoming a challenging issue in PoC. To maintain a patient's privacy, the biological data should be well restrained i.e. from the endurance of malicious activities [35].

Generally speaking, it is classified into three system components such as sensor, network, and computing. These elements are used to sense, actuate, and monitor the environmental behavior that forms a heterogeneous network to communicate with the mobile terminals. Later, the network configuration transmits the data to offer application services to remote PoC. Of late, IoT-based remote PoC has been considered as an intelligent unit for telematics services. Due to serious health hazards in chronic and cardiovascular diseases, the demand for remote PoC has gained the researches attention and medical institutes. This provides a supplementary access to the medical institute, where the medical doctors collect and examine the physiological data of patients to monitor periodically.

1.2 Research motivation

Big data and AI play a crucial role to facilitate the preparedness of COVID-19 including screening, tracing, testing, treating. It uses a dedicated framework including migration map, smartphones, electronic payments, and social media to monitor the activities of the people. It may also allow tracking the people movement to forecast the transmission regions. Moreover, the integrated framework provides a privilege to infer the travel histories of the common people. In modern healthcare, the potential use of AI technique accelerates the process of intelligent and autonomous to regulate the system compliance requirements. Significant computing considers the learning process to investigate the structured datasets such as genetic and imaging data. It uses machine learning to build an investigation algorithm to collect the data features. However, the investigation techniques are still vulnerable to potential threats to critical application systems such as digital forensic and biometric. Therefore, a well-established protocol called authentication and key-agreement (AKA) [10] is highly necessitated to attain the basic security requirements of AKA namely user untraceability, forward/backward secrecy [27] and user anonymity [46]. Lamport introduced the initial key authentication mechanism [23] in 1981. In 1991, Frank et al. [43] presented a key agreement protocol that completely relies on HTTP. Conversely, Yang et al. [41] presented that Frank et al. were uncertain to withstand the vulnerabilities such as redirection, replay attack, and man-in-the-middle. Yang et al. constructed a competent user authentication, which resolves the key issues of Frank et al. Of late, several authentication mechanisms, namely two-factor [41], three-factor [11], identity-based [8], etc. have been constructed using pairing-based, factoring and discrete logarithm, elliptic-curve (EC) cryptography [22], and chaotic-map [40].

Though, these protocols experience a serious security limitation. The extensive investigation shows that most of the authentication mechanisms do not have proper cryptographic primitives or have a design defect to meet the security goals. Awasthi et al. [3] determined that Shen et al. [36] is easily susceptible to key-impersonation attack. To deal with the issues of Shen et al., Awasthi et al. constructed a novel timestamp-based authentication protocol. Though, their protocol discloses the information of the smart devices and its related parameter details to the adversaries. Additionally, Huang et al. [19] exhibited that Awasthi et al. cannot be resilient to user impersonation attacks and failed to maintain the secret-key /password update phase. Also, they introduced an improved timestamp-based authentication mechanism to resist various potential threats such as redirection, replay, password guessing, etc. Amin

et al. [2] pointed out that Huang et al. cannot withstand key impersonation, password-guessing (online/offline) and privilege-insider. To solve security issues and inefficiency of the password update phase, Amin et al. presented a secure authentication based on the RSA cryptosystem. Computing devices and network technologies have developed various Internet of Things (IoT) application systems such as sustainable smart systems. It creates a real-world that seamlessly integrates the physical objects to communicate autonomously over the Internet.

Numerous authentication and key agreement mechanisms [16, 27] have been introduced for resource-constrained electronic healthcare application systems. It may apply several cryptographic operations including Rivest-Shamir-Adleman (RSA) cryptosystem (i.e. an exponential operation), Chebyshev polynomial (i.e. chaotic one-way hashing operation), etc. A security protocol based on chaotic-map shows better performance efficiencies in comparison with conventional cryptosystem namely RSA and public-key cryptography. In most cases, ECC and RSA based authentication protocols consume more computation overhead because of excessive operators such as point multiplicative or modular exponential. It is evident that the secret key size of the Chebyshev Chaotic - Map is more modest as compared to ECC and RSA. Hence, it is widely identified to be chaotic-map based authentication schemes to achieve less computation and communication efficiencies than ECC or RSA-based authentication protocol. Many chaotic-map based authentication protocols are susceptible to desynchronization [41] and denial-of-service (DoS) attack [11]. Moreover, their schemes cannot offer client anonymity [46] and revocation mechanism for stolen or lost smartcard [11]. Additionally, the existing authentication schemes do not concentrate on real-time scenarios to examine ephemeral or temporary leakage that may cause a serious threat to security design.

The above key issues propose to incorporate less computation and lightweight authentication based on a chaotic-map in RM-PoC. It can achieve better security efficiencies as compared to other existing schemes. As a result, the proposed scheme introduces single user sign-in to prevent the susceptibilities, such as password-guessing (online/offline), key-impersonation etc. However, a smartcard verifier attack i.e. lost/stolen is still challenging to address. Also, Srinivas et.al. [37] considered a symmetric authentication for WMSN. However, their protocol utilizes only less computation operations to attain lightweight key attributes that are formally analyzed to validate the threats such as man-in-the-middle and replay. Correspondingly, [4, 28] influenced security testing using AVISPA i.e. Automated Validation of Internet Security Protocols and Applications to validate the network threats. The recent published researches [1, 12] preferred to utilize efficient user authentication schemes that verify the performance of the Internet of Things (IoT). Turkanovic et al. [38] suggested a novel key agreement scheme for a distributed environment. Inopportunely, their authentication scheme has several security weaknesses, which are motivated to uncategorized cryptographic attacks. Farash et al. [14] resolved the security weaknesses of Turkanovic et al. Also, they suggested an enhanced authentication mechanism.

1.3 Research motivation

The major research contributions are as follows:

1. The proposed SUSI permits remote-user to strongly exchange a session key to any available medical-sensor node. It employs a privacy-preservation mechanism, where proper mutual authentication can be ensured between the real-time entities.

2. It practices only simple hashing and X-OR computation to reduce the computation cost and introduces formal analysis to prove the efficiency of the proposed SUSI.
3. In this study, Chebyshev Chaotic-Map operations, namely multiplication and addition are applied to achieve the secret key authentication.
4. In order to reduce the computational overhead, a Chebyshev Chaotic-Map based authentication substitutes two-point multiplication into one modular-inversion and point-multiplication, whereby Chebyshev Chaotic-Map operations is claimed to be faster than the traditional operations [40].
5. Lastly, a security analysis including formal using RoR is conducted to show the major significance of the proposed SUSI scheme that demonstrates the security protection against the potential attacks required in RM-PoC.

Section 2 discusses the related works and intelligent architecture using a cloud of things. Section 3 explains the Chebyshev Chaotic-Map and adversarial model. Section 4 proposes a single user sign-in (SUSI) mechanism using Chebyshev Chaotic-Map to describe the significance of system protection. Section 5 shows the security and performance analysis of the proposed SUSI and existing authentication schemes. Section 6 demonstrates the network simulation to analyze the quality metrics such as transmission delay, throughput rate, and packet delivery ratio. Section 7 concludes the research work.

2 Background

This section discusses the related works and intelligent architecture using a cloud of things to signify the challenging issues of existing authentication schemes.

2.1 Related works

Most of the countries prefer to use the web and cloud-based applications to support effective screening to the individuals. It adopts a high-performance camera to capture the people's thermal images that measure their body temperatures at public transport, hotels workplace, and shopping malls. The collection of data is utilized to identify the hotspots and infection clusters that make conform to the testing and treatment process. Lately, researchers and business experts have been attracted to a protuberant solicitation of Wireless Medical Sensor Networks (WMSNs). It is encompassed of numerous lightweight smart devices with limited storage space, less computation power and bandwidth. Some investigation groups and schemes have concentrated their studies on smart patient monitoring. It uses wireless sensor networks (WSNs) to perform a live patient healthcare monitoring [5]. In structural design, medical sensors are firstly located on the victim physical structure to sense and gather the physiological data of patients, such as heart rate, human body temperature. In general, sensing data are conglomerated over real-time using smart devices by medical specialists. Conversely, the outflow of detecting data may impinge a victim's data privacy and the interruption has the prospect to induct data alteration. It can give rise to the wrong diagnosis. Unlike traditional sensor network systems, the detected and collected victim's data are very delicate. Therefore, the insecure communication over a wireless channel is exceptionally essential [35].

Numerous authentication protocols [32] have common security weaknesses, such as proper mutual authentication, data freshness, sensing data forgery, data disclosure, privileged-insider and key-impersonations attack. To address the security issues, the existing authentication schemes such as Chen et al. [6] and Le et al. [24] were enhanced. Conversely, their scheme cannot resist the security threats such as key-impersonation and replay, whereas Le et al. cannot offer the property of proper mutual authentication [7]. In this work, to support the security issues for WMSN further, an IEEE standard of 21,451–2 [15, 20] is preferred. The integration component known as Application Programming Interface (API) methods is useful, which uses an access controller to sense the records accurately in any intelligent system via WMSN. Likewise, an enhanced remote authentication using smart devices was offered to claim that their scheme can prevent password-guessing attacks i.e. online/offline [39]. Additionally, their scheme holds client anonymity to prevent information outflow. On the other hand, their scheme cannot resist the property of user anonymity; and thus does not prevent offline password guessing, information outflow and stolen-verifier [33].

Odelu et al. [33] introduced an authentication protocol based on ECC that shows the formal and informal security analysis to prove the security efficiency. However, their scheme cannot prevent offline password-guessing, and stolen-verifier attack. Moreover, they were failed to examine the performance overhead including computation and communication. Importantly, their algorithm did not use the hash properties explicitly. An efficient and adaptive mutual authentication framework was proposed [24] to suit real-time heterogeneous applications. In their mechanism, the phases such as system initialization; dynamic key sharing and establishment; revocation; and addition of new communication node are contrived. Liu et al. [29] presented a privacy-preserving authentication with shared authority that addresses the privacy of cloud-storage. Jiang et al. [21] developed a three-factor privacy preservation for e-Health cloud that incorporates a user revocation phase to improve the security efficiencies.

Yu et al. [44] proposed an ID-based authentication with remote server integrity that reduces the system complexity and computation cost. Hu et al. [18] improved the privacy preservation scheme to examine the processing capacity and bandwidth consumption. Gunasinghe et al. [17] proposed a privacy-preserving biometric-based authentication for smart devices. Liu et al. [30] aimed to design a cooperative privacy preservation that considers space-ware and time-aware contexts. Li et al. [26] improved the mutual authentication and privacy preservation protocol that protects the privacy of the medical data to guarantee system reliability. Deebak et al. [12] developed an authentic-aware privacy preservation for the smart e-Health system. Madhusudhan et al. [31] designed an efficient authentication protocol to secure the roaming networks. However, most of the existing authentication schemes [12, 17, 18, 26, 30, 31, 44] could not provide better security and performance efficiencies to prevent potential attacks. Table 1 reviews the challenges of existing authentication schemes.

2.2 Proposed 5G framework

Figures 1 illustrates a proposed 5G framework for smart medical intelligence. The proposed 5G framework incorporates various real-time components such as medical information systems, 5G network, cloud service, and wearable sensors to understand the functional performance of healthcare systems. Each component has its own significance to monitor and analyze the potential threats. Wearable sensors collect and store the clinical data of the patient in medical information systems. The medical systems apply the smart intelligence

Table 1 Challenges of Existing Authentication Schemes

Existing Scheme Based on Privacy Preservation	Key Agreement Properties							Security Attacks					
	CH_1	CH_2	CH_3	CH_4	CH_5	CH_6	CH_7	CH_8	CH_9	CH_{10}	CH_{11}	CH_{12}	CH_{13}
Liu et al. [29], 2014	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*
Jiang et al. [21], 2016	*Yes*	*No*	*No*	*Yes*	*No*	*No*	*Yes*	*No*	*Yes*	*Yes*	*Yes*	*No*	*No*
Yu et al. [44], 2016	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*
Hu et al. [18], 2017	*No*	*Yes*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*
Gunasinghe et al. [17], 2017	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*
Liu et al. [30], 2018	*Yes*	*No*	*No*	*No*	*No*	*No*	*Yes*	*No*	*No*	*No*	*No*	*No*	*No*
Li et al. [26], 2018	*Yes*	*No*	*No*	*Yes*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*
Deebak et al. [12], 2019	*Yes*	*Yes*	*No*	*Yes*	*Yes*	*No*	*No*	*Yes*	*No*	*Yes*	*No*	*No*	*Yes*
Madhusudhan et al. [31], 2020	*Yes*	*No*	*No*	*Yes*	*Yes*	*No*	*Yes*	*No*	*Yes*	*No*	*Yes*	*Yes*	*No*

CH_1 Property of Proper Mutual Authentication, CH_2 Property of Secure Session-Key, CH_3 Property of Known-Key Agreement, CH_4 Property of User-Anonymity, CH_5 User Friendliness, CH_6 Property of Secret Key Disclosure, CH_7 Property of Perfect Forward Secrecy, CH_8 Resilient Stolen Smart Card Attack, CH_9 Resilient to Password-Guessing Attack, CH_{10} Resilient to Stolen-Verifier Table Attack, CH_{11} Resilient to Privileged-Insider Attack, CH_{12} Resilient to Key-Impersonation Attack, CH_{13} Resilient to Sensor Node Capture Attack.

on the technical data to detect the symptoms caused in terms of threat and non-threat. Cloud service includes policy certification and authentication access that interconnects the infrastructure over the Internet to upload the real-time data. It can observe the threat data to

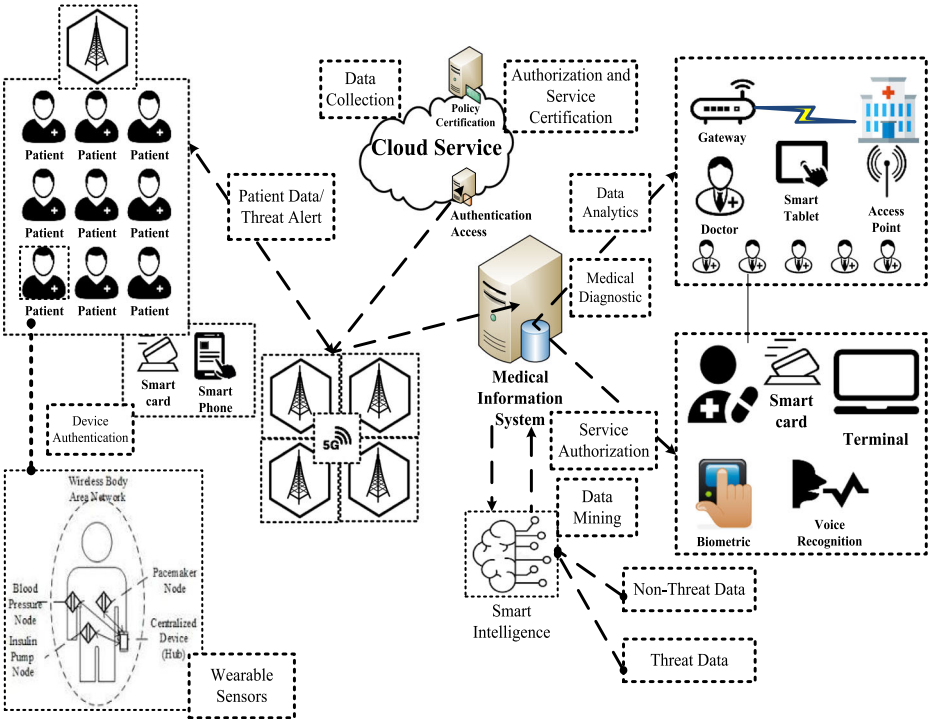

Fig. 1 Proposed 5G Framework for Smart Medical Intelligence

perform the following actions: 1. Infer the patient's condition, 2. Generate a prediction result, 3. Communicate the result with medical experts, and 4. Provide a storage space for treatment follow-up. It includes a smart intelligence system using 5G that integrates wearable sensors, smartphones, and medical information systems in healthcare services. It utilizes low cost and low-power wireless devices such as Bluetooth, ZigBee, WiFi, and 6LoWPAN to provide connectivity between wearable sensors and smartphones. In another view, 5G is widely deployed to associate smartphones with cloud services and dedicated medical information systems to collect and analyze the sensing data of the patients. In healthcare, the biological sensors estimate the physiological conditions of the patient that feed the patient's information. to the smart intelligence system whereby the data are analyzed through the knowledge of healthcare service providers. It can infer the data in the form of threat or non-threat over public Internet access to gain the information services. It has a dedicated data storage server to store and analyze the protected health information (PHI) of patients that grant the policies and service authentication governed by the Upon the successful authentication, the server utilizes the data blocks consisting of patient info, media-expert, authentic server over TMIS [42].

In the healthcare system, the medical patients obtain the PHI to screen the patient's health condition, which is very much useful to provide a medical prescription [25]. In an emergency, a smart intelligent service can be initiated to offer medical treatments to the casualties before he/she undergoes any standard operating procedure. Importantly, the research and development process intensively analyzes the sensor input/output to foresee the network threats and its countermeasures.

The practical key properties of WMSN [27, 37] are enumerated as follows:

Proper Mutual Authentication: The experts agree to ensure a proper authentication between the expert, authentic-gateway, and sensor-node to approve the service access.
Secret Session-Key Agreement: Segments the key parameters to generate a unique session-key among the communication entities to protect the system over an insecure network.
Known-Key: A_{dv} wishes to interfere with the secure session-key of any user, then he/she cannot easily infer a proper computation to compromise the session-key of the legal entities.
Client Anonymity: User identities, such as an expert/device and remote-server may be concealed to prevent authorized access over public networks.
Stolen Smartcard Attack: A_{dv} modifies the user password upon the inference of old password and user identity in the session-key update phase to validate whether the entries are valid to change the secret-key or not.

To address the aforestated issues, an ECC-based authentication was constructed for the WSNs [22]. Since they have more computation and storage complexity, it cannot be suitable for any intelligent systems [12]. Generally, users may usually desire to practice laidback to-recollect the system parameters, such as key characteristics and secret-key to gain the system access [1]; and thus client anonymity cannot be offered [46]. In the analysis, the anonymous based authentication protocols are vulnerable to user anonymity, password-guessing i.e. offline and de-synchronization attacks [46]. In order to provide reliable security and privacy, this paper proposes a SUSI Mechanism that secures the intelligence systems.

3 Preliminaries

This section discourses the Chebyshev Chaotic-Map and adversarial model to explain its major importance in any wireless communication system. The important key parameters of the proposed single user sign-in (SUSI) are illustrated in Table 2.

3.1 Mathematical assumption of Chebyshev chaotic-map

This assumption defines the Chebyshev chaotic-map that represents a Chebyshev polynomial $T_n(x)$, where $\langle x \rangle$ is a degree of $\langle n \rangle$. It can be defined as:

$T_n(x) = \cos n\theta$, where $x = \cos \theta$.

This assumption also defines the recurrence relation $T_n(x)$, which can be expressed as:

$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x)$, for any $n \geq 2$ with the assumption of $T_0(x) = 1$ and $T_1(x) = x$

This assumption also defines the semi-group property of Chebyshev polynomial to satisfy the given expression:

$T_r(T_s(x)) = T_{sr}(x) = T_s(T_r(x))$, for $s, r \in Z^+$

This assumption also defines the chaotic property of Chebyshev polynomial, where $n > 1$ represents a polynomial map $T_n : [-1, 1] \rightarrow [-1, 1]$ for the degree $\langle n \rangle$ with its relevant invariant density:

$f^*(x) = {}^1/_{\left(\pi.\sqrt{(1-x^2)}\right)}$, for an exponent of Lyapunov i.e. $\ln n > 0$ [45]

Dharminder et al. [13] improved the authentication protocol using Chebyshev chaotic-map to prevent the security weakness demonstrated by the existing protocols [26, 30]. To reinforce the security strategies, the Nergamo et al. extended the Chebyshev polynomial to satisfy the properties of semi-group and commutative i.e. in the interval of $\langle -\infty, \infty \rangle$. The expression is as follows:

$$T_n(x) \equiv 2xT_{n-1}(x) - T_{n-2}(x) \ mod \ q,$$

Table 2 Important Parameters Used in SUSI

Parameters	Description
A_{dv}	Adversary
M_S	Medical Sensor
M_D	Medical Device
R_S	Remote Server
GW_A	Gateway Access
$T_n(x)$	Recurrence Relation
q	Large Prime Integer
$\langle x \rangle$	A Polynomial Element
SS_k	secret session key with a string length k
PK_S	public-key
I_d	Device-Identity
ID_{MS}	Identity of M_S
PWD_{MS}	Password of M_S
ID_{R_S}	Identity of R_S
$h(.)$	One-way hash function i.e. $h : \{0,1\}^* \rightarrow \{0,1\}^{l_g}$
$H(.)$	One-way hash function i.e. $H : \{1,-1\}^* \rightarrow \{0,1\}^{l_g}$
$E_K(.)$, $D_K(.)$	Symmetric encryption /decryption with a string length K
MSG_1 To MSG_4	Transmission messages

Where $n \geq 2, \forall\, x \in \langle -\infty, \infty \rangle$ and q is a large prime integer. It can be further defined as:

$$T_r(T_s\ (x)\ ) = T_{sr}(x) = T_s(T_r\ (x)\ )\ mod\ q$$

This improved Chebyshev chaotic-map shows the assumptions of discrete logarithm and Diffie Hellman [22, 40]. The assumption problems are:

Extended Chebyshev chaotic-map based discrete-logarithm problem (DLP) Assume that x, y and p are the integers to determine the parameter $\langle r \rangle$ that is much helpful to satisfy $y = T_r(x)\ mod\ p$ i.e. computationally infeasible. The major advantage is that the adversary A_{dv}^{DLP} may try to resolve the extended Chebyshev chaotic-map based *DLP* i.e. computationally insignificant.

Extended Chebyshev chaotic-map based computational Diffie Hellman problem (CDHP) Assume that $T_r\ (x)$, $T_s\ (x)$, $T(.)$, x and p where $r, s \geq 2$, $x \in \langle -\infty, \infty \rangle$ and p is a large prime integer to calculate:

$T_{rs}(x) \equiv T_r(T_s\ (x)\ ) \equiv T_s(T_r\ (x)\ )\ mod\ p$, which is computationally infeasible to solve the extended Chebyshev chaotic-map based Computational Diffie Hellman problem, denoted as A_{dv}^{CDHP}. Hence, it is considered to be insignificant.

Extended Chebyshev chaotic-map based decisional Diffie Hellman problem (DDHP) Assume that the parameters such as $T_r\ (x)$, $T_s\ (x)$, $T(.)$, x and p are considered to decide:

$T_{rs}(x) \equiv T_z(x)\ mod\ p$, which is considered to be hold or computationally infeasible. The advantage is that an adversary can solve the extended Chebyshev chaotic-map based decisional Diffie Hellman problem, denoted as A_{dv}^{DDHP}. Therefore, it is computationally negligible.

3.2 Attacker model

Most of the e-Health systems preserve the patient medical information from the outside environment that ensures the safety of the human being. To provide a timely diagnosis, the communication entities namely a patient and doctors are nowadays utilizing smart devices. The prime objective is to implant the medical sensors on a patient's body that monitor and analyze the health status over a wireless channel. Since medical devices are highly exposed to network threats, an unauthorized user may try to steal sensitive data. Due to the physical stimuli, the global opportunists including media, insurance companies, etc. are seeking an opportunity to gain information access. As referred to in [12], an adversary A_{dv} is assumed to have the following abilities to test the scenario i..e. formal and informal.

1. A_{dv} may try to overhear or eavesdrop the data transmission over public channel access i.e. between the legal user and remote server under the three-factor system environment.
2. A_{dv} may wish to steal the user's particulars e.g. smartcard or mobile-device in order to retrieve the confidential information from the stolen device.

3. A_{dv} cannot infer the confidential parameters such as random integer, hash function and private secret-key s_k from the remote server R_S within the execution of polynomial time. It is presumed that the above computation could at least achieve a minimum-security length.
4. A_{dv} may deduce the communication parameters such as secret password and user identity from the two finite sets. Therefore, A_{dv} has the possibility to perceive the above information in the given polynomial time.
5. A_{dv} may try to deceive the remote server R_S to know the confidential information i.e. specifically to enact or behave as a genuine user.
6. A_{dv} may try to perceive or guess a low entropy i.e. identity or password apart from others. However, the rules of the polynomial equation may not be violated to reveal the confidential data i.e. identity or secret password at the same execution time. Assume that the user identity length and secret password has n for each parameter to derive the probability $1/2^{6n}$ i.e. for n character long-string.
7. To achieve the property of forward secrecy demonstrated in [46], A_{dv} may try to collect the long-term information including user identity, secret password, storage data and a remote server. Though A_{dv} perceives the above confidential data, he/she cannot compute the previous session. Thus, this proposed mechanism satisfies the property of forward secrecy.

4 Proposed single user sign-in (SUSI) mechanism

This section presents a proposed SUSI mechanism that is completely constructed using extended Chebyshev chaotic-map. As secret session-key is constructed using *CDHP*, none of adversary A_{dv} can precompute the secret session-key. In other words, as the proposed scheme is based on Chebyshev's chaotic-map, a malicious adversary may not compute a shared session-key to establish a communication between the user and remote server to forge a valid request message or impersonate as an authorized user. Moreover, in the phase of the secret-key update of SUSI, the random identities always guarantee the data freshness to authorize the data from the access of remote-server. Thus, the proposed SUSI can prevent the user privileged access to resist the susceptibilities, such as redirection, replay, and denial-of-service (DoS) attack. This proposed scheme comprises of: initialization, registration, login and key authentication, and secret-key update. The initialization phase uses Chebyshev chaotic-map to invoke a parameter of $\langle x \rangle$ on the given interval $(-\infty, \infty)$ that wants a large prime integer $\langle p \rangle$ to perform a modular arithmetic operation in order to maintain secrecy during the system initialization phase. Assume G, g *and* q be the defined parameters of the group. In addition, a secret session key SS_k, $SS_k^{'}$(Conjugate of SS_k) and registration server R_S (Which maintains SS_k with a random string length k) are chosen. Assume $H: \{0,1\}^* \rightarrow \{0,1\}^k$ defines a hash function which resists the target collision and $PRF_{S_k} : \{0,1\}^k \rightarrow \{0,1\}^k$ defines a pseudo-random function key. In addition, we define a hash (conjugate) function $H^{'}: \{0,1\}^* \rightarrow \{0,1\}^k$ to preserve the identities of the users. In SUSI scheme, SS_k is assumed to be a derivative key by the $H(SS_k)$.

System initialization phase Remote-server R_S builds a system communication parameters to perform the following execution steps:

Step 1: R_S generates a random prime number q and selects a polynomial element $\langle x \rangle$ for Chebyshev polynomial $T_n(x)$

Step 2: R_S chooses a random one-way hash $H(.)$ to perform symmetric encryption and decryption i.e. $E_K(.)/D_K(.)$

Step 3: R_S chooses a secret session key $SS_k \in \langle 1, q+1 \rangle$ to compute the public-key $PK_S = T_S(x) \bmod q$

Step 4: R_S publishes the system parameters i.e. $\{q, x, PK_S, H(.), E_K(.), D_K(.)\}$

System registration phase R_S issues a secure gateway to the medical sensor M_s to ensure string security and privacy over a secure channel. M_s wishes to exchange SS_k to register with R_S.

Step 1: M_s sends a device-identity I_d along with user identity ID_{MS} to R_S. R_S verifies whether $M_s$is already registered or not. Otherwise, M_s computes $X_A = H(I_d \| ID_{MS} \| SS_k)$ and stores the system parameters $\{q, x, X_A, SS_k, H(.), E_K(.), D_K(.)\}$ in R_S. It delivers the parameters to GW_A over a secure channel.

Step 2: GW_A receives the significant parameters from M_s to gain the server access R_S. GW_A collects the M_s inputs such as ID_{MS} and $PWD_{MS}$to compute $G_A = H(ID_{MS} \| PWD_{MS} \| I_D) \oplus X_A$; and $M_A = H(ID_{MS} \| I_D \| X_A)$. Lastly, it stores the system parameters $\{q, x, G_A, M_A, H(.), E_K(.), D_K(.)\}$ in the storage device.

System login and key-authentication phase User namely M_s enters a secret session-key to access the private information of patient. A secure gateway retrieves the value of the secret session-key to perform the following computation [as shown in Fig. 2]:

Step 1: M_s connects the medical device M_D that considers the device inputs such as ID_{MS}, and PWD_{MS}. G_A computes:

$$X_A^* = G_A \oplus H(ID_{MS} \| PWD_{MS} \| I_D);\ M_A^* = H\left(ID_{MS} \| PWD_{MS} \| I_D \| X_A^*\right)$$

When M_A is not equaled to M_A^*, GW_A aborts the service session. Otherwise, GW_A chooses any random value $SS_k \in \langle 1, q+1 \rangle$ to compute $PK_A = T_{SS_k}(x) \bmod q$; $PK_{AS} = T_{SS_k}(K_S) = T_{MS}(x) \bmod q$; $Y_{MS} = H(ID_{MS} \| I_D \| PK_{AS} \| X_A)$; and $Z_{MS} = E_{K.SS_k}(ID_{MS}, I_D, Y_{MS})$. Finally, M_s sends the transmission message $MSG_1 = \{Z_{MS}, PK_A\}$ to GW_A.

Step 2: Upon receiving the message MSG_1 from M_s, GW_A connects with R_S to access the input parameters such as ID_{R_S} and PWD_{R_S}. Then, it computes:

$$X_{R_S}^* = G_{R_S} \oplus H(ID_{R_S} \| PWD_{R_S} \| I_D);\ M_{R_S}^* = H\left(ID_{R_S} \| PWD_{R_S} \| I_D \| X_{R_S}^*\right)$$

When M_{R_S} is not equaled to $M_{R_S}^*$, GW_A aborts the service session. Otherwise, GW_A chooses any random value $SS_k \in \langle 1, q+1 \rangle$ to compute $PK_{R_S} = T_{SS_k}(x) \bmod q$; $PK_{AS} = T_{R_S}(K_S) = T_{AS}(x) \bmod q$; $Y_{MS.R_S} = H(ID_{R_S} \| I_D \| PK_{R_S} \| X_A)$; $Z_{R_S} = H(ID_{R_S} \| Y_{MS.R_S})$; and $Z_{R_S.SS_k} = H(ID_{R_S} \| PK_{R_S} \| PK_A \| X_A)$; and $Z_{R_S} = E_{K.R_S}(ID_{R_S}, I_D, Z_{R_S}, Z_{R_S.SS_k})$.

Then, it sends the transmission message $MSG_2 = \{Z_{MS}, PK_A, Z_{R_S}, PK_{R_S}\}$ to R_S.

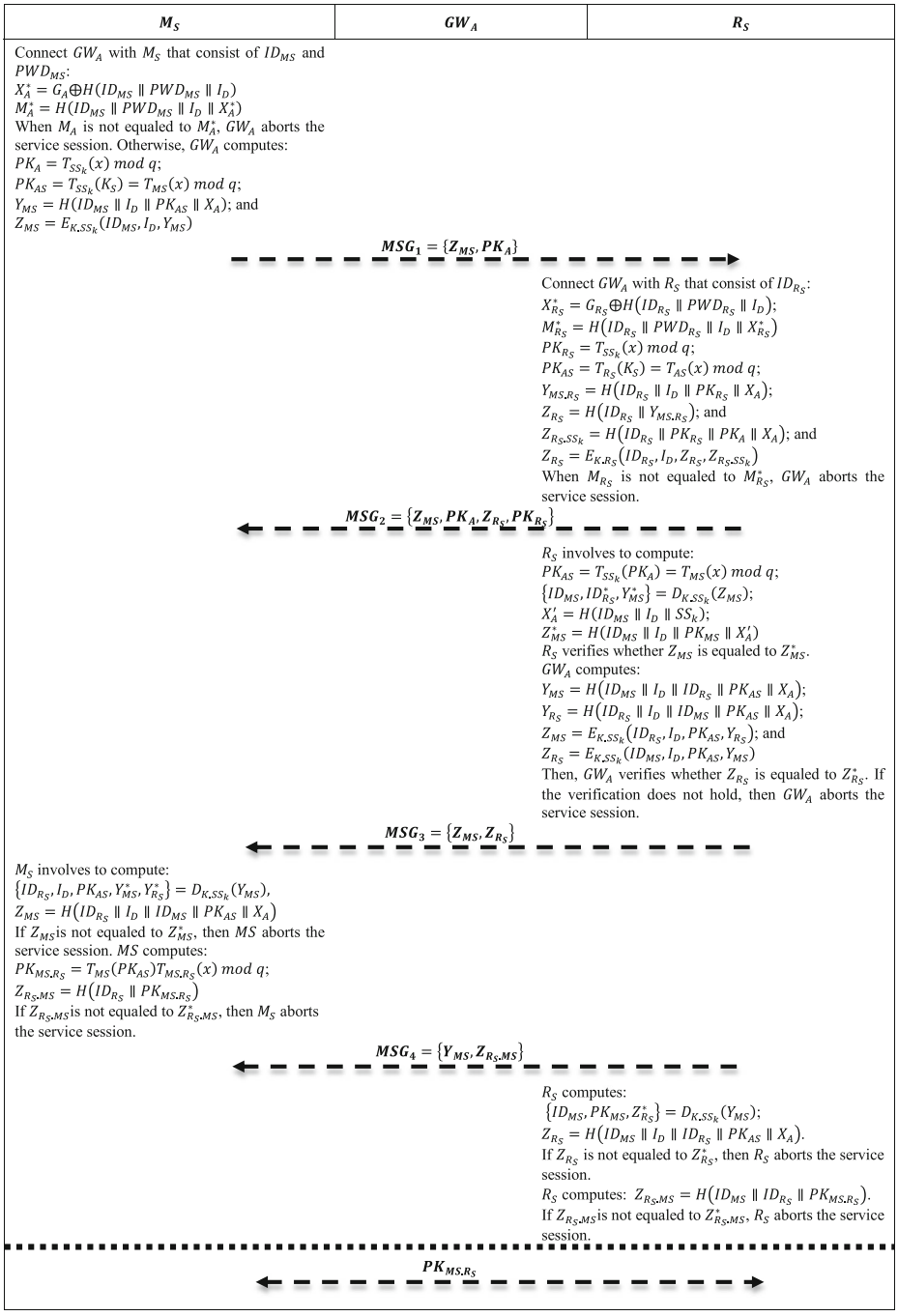

Fig. 2 Flow Structure of Proposed SUSI: Login and Authentication Phase

Step 3: Upon receiving the message MSG_2 from GW_A, R_S involves the following computation: $PK_{AS} = T_{SS_k}(PK_A) = T_{MS}(x)\ mod\ q$; $\left\{ID_{MS}, ID^*_{R_S}, Y^*_{MS}\right\} = D_{K.SS_k}(Z_{MS})$; $X^{'}_A = H(ID_{MS} \| I_D \| SS_k)$; $Z^*_{MS} = H\left(ID_{MS} \| I_D \| PK_{MS} \| X^{'}_A\right)$. Then, R_S verifies whether Z_{MS} is equaled to Z^*_{MS}. If the verification does not hold, then R_S aborts the service session.

Also, GW_A computes:

$PK_{R_S} = T_{SS_k}(PK_{R_S}) = T_{R_S}(x)\ mod\ q$; $\left\{ID_{R_S}, ID^*_{MS}, Y^*_{R_S}\right\} = D_{K.SS_k}(Z_{R_S})$; $X^{'}_A = H(ID_{R_S} \| I_D \| SS_k)$; $Z^*_{R_S} = H\left(ID_{R_S} \| I_D \| PK_{R_S} \| X^{'}_A\right)$. Then, GW_A verifies whether Z_{R_S} is equaled to $Z^*_{R_S}$. If the verification does not hold, then GW_A aborts the service session. Also, GW_A verifies:

$Y_{MS} = H(ID_{MS} \| I_D \| ID_{R_S} \| PK_{AS} \| X_A)$; $Y_{R_S} = H(ID_{R_S} \| I_D \| ID_{MS} \| PK_{AS} \| X_A)$; $Z_{MS} = E_{K.SS_k}(ID_{R_S}, I_D, PK_{AS}, Y_{R_S})$; and $Z_{R_S} = E_{K.SS_k}(ID_{MS}, I_D, PK_{AS}, Y_{MS})$. Lastly, GW_A sends the transmission message $MSG_3 = \{Z_{MS}, Z_{R_S}\}$ to M_S and R_S.

Step 4: After receiving the message $MSG_3$from GW_A, M_S involves the following computation:

$$\left\{ID_{R_S}, I_D, PK_{AS}, Y^*_{MS}, Y^*_{R_S}\right\} = D_{K.SS_k}(Y_{MS}), Z_{MS} = H(ID_{R_S} \| I_D \| ID_{MS} \| PK_{AS} \| X_A)$$

If $Z_{MS}$is not equaled to Z^*_{MS}, then MS aborts the service session. MS computes:

$PK_{MS.R_S} = T_{MS}(PK_{AS}) T_{MS.R_S}(x)\ mod\ q$; $Z_{R_S.MS} = H(ID_{R_S} \| PK_{MS.R_S})$

If $Z_{R_S.MS}$is not equaled to $Z^*_{R_S.MS}$, then M_S aborts the service session. Otherwise, M_S sets $PK_{MS.R_S}$ as a session key. M_S computes $Z_{R_S.MS} = H(ID_{MS} \| ID_{R_S} \| PK_{MS.R_S})$. M_S sends the transmission message $MSG_4 = \{Y_{MS}, Z_{R_S.MS}\}$ to R_S.

Step 5: After receiving the message $MSG_4$from M_S, R_S computes $\{ID_{MS}, PK_{MS}, Z^*_{R_S}\} = D_{K.SS_k}(Y_{MS})$; $Z_{R_S} = H(ID_{MS} \| I_D \| ID_{R_S} \| PK_{AS} \| X_A)$. If Z_{R_S} is not equaled to $Z^*_{R_S}$, then R_S aborts the service session. R_S computes $Z_{R_S.MS} = H(ID_{MS} \| ID_{R_S} \| PK_{MS.R_S})$. If $Z_{R_S.MS}$is not equaled to $Z^*_{R_S.MS}$, R_S aborts the service session. Otherwise, R_S sets $PK_{MS.R_S}$ as a session key.

System key update phase The execution steps are as follows:

Step 1: M_S connects GW_A that collects the inputs such as ID_{MS}, $ID_{R_S}$and PWD_{MS} to compute $X_A = G_A \oplus H(ID_{MS} \| PWD_{MS} \| I_D)$; and $M_A = H(ID_{MS} \| I_D \| X_A)$ to verify whether M_A and M^*_A are identical. Otherwise, GW_A terminates the service session. Step2: R_S connects GW_A to render a new $PWD^{New}_{MS}$to compute $G^{New}_A = H\left(ID_{MS} \| I_D \| PWD^{New}_{MS}\right) \oplus X_A$ and $M^{New}_A = H\left(ID_{MS} \| I_D \| PWD^{New}_{MS} \| X_A\right)$. Eventually, GW_A changes the parameters $\langle G_A, M_A \rangle$ into $\left\langle G^{New}_A, M^{New}_A \right\rangle$.

5 Analysis model

This section demonstrates the analysis model using the RoR model [3] to strengthen the efficiency of the proposed SUSI scheme. Moreover, the security analysis including formal and informal proves that the proposed SUSI may prevent several potential vulnerabilities to enhance the security competences.

5.1 Formal analysis

The formal analysis shows that the assumptions of Chebyshev chaotic-map are employed to prove the mathematical numerals are inflexible. Two random-oracle is enforced to prove the importance of secret-key [22, 40], which can be preserved from the adversaries. The proofs of execution are:

Reveal (1) RoR model may yield a secret session-key SS_k to perform the executed output $PK_{MS.R_S} = T_{MS}(PK_{AS})T_{MS.R_S}(x)\ mod\ q$ to validate the authentication request.

Reveal (2) This RoR model uses two system parameters $\lambda\ and\ Q_1$ to yield the users's context-identity $Q_1 = T_n(x)\ mod\ p$ and $\lambda = T_n(T_m(x))\ mod\ p$

Theorem 1 *Consider that the proposed SUSI is officially protected to defend the common secret session-key Q_2 of gateway-node and device/sensor, if the proper statement of Chebyshev chaotic-map is provably intractable.*

Proof An adversary A_d who tries to generate a secret session-key of the authorized user SS_k and device identity M_d during the login and authentication phase. In case of *Reveal* (1) and *Reveal* (2), the system authentication phase is accessed to perform and deduce common session-key. To demonstrate the possibility of success proportion $Prob1_{MS.R_S\ Ad}^{EC-DLP}$, where an extended Chebyshev chaotic-map based *DLP* is a oracle model secret key, $Success1_{MS.R_S\ Ad}^{EC-DLP} = |2_{Pr}\left[Prob1_{MS.R_S\ Ad}^{EC-DLP} = 1\right] - 1|$ is defined to experiment $Ad1_{MS.R_S\ Ad}^{EC-DLP}(Y_{MS}, Z_{R_S.MS}) = Max_{A_d}\left(Success1_{MS.R_S\ Ad}^{EC-DLP}\right)$, where the probability of maximum success rate is measured over A_d act through the execution time t_1 and demands $P_{R1}\ and\ Q_{R2}$ to disclose the RoR model *Reveal* (1) and *Reveal* (2). The proposed SUSI scheme is legitimately identified to be protected as compared to adversary A_d particularly to guard the mutual secret session-key SS_k between M_S/R_S and GW_A, if $Ad1_{R_S.MS\ Ad}^{EC-DLP}(Y_{MS}, Z_{R_S.MS}) < \varepsilon$, to some extent $\varepsilon > 0$.

With the experimental statement of $Prob1_{R_S.MS\ Ad}^{EC-DLP}$, an adversary A_d can gather the identifications of expert, such as $ID_{MS}, PK_{MS}, Z_{R_S}^*$ to make it in his / her game, if he / she has the ability to resolve the problem of extended Chebyshev chaotic-map based discrete-logarithm problem to control a numerical integer R_i, where $R_i \in F_p^*$. Conversely, this assumption is computationally unpractical owing to the difficulties defined As the computational step of adversary is commonly limited on $Ad1_{Ad,E_K(.)}^{EC-DLP}(t)$ and $Ad1_{Ad}^{R_i}(t)$, the adversary has $Ad1_{R_S.MS\ Ad}^{EC-DLP}(Y_{MS}, Z_{R_S.MS}) < \varepsilon$, for any insufficiency $\varepsilon > 0$. Therefore, this SUSI scheme can

adhere to the security properties namely proper mutual authentication and secret session-key agreement in contrast to any *Ad*.

Theorem 2 *Consider that the proposed SUSI scheme is rightfully safeguarded to keep the system parameter Q_2 of theM_S/R_S* and *GW_A, even if the expert M_S or smart device M_D is stolen.*

Proof Building an adversary A_{dv}, who ought to derive the record of expert M_D to disclose. This aforesaid statement assumes that M_D's is stolen. As referred to in [36], A_{dv} applies the approach of power-analysis to infer the storage information of M_D, such as$\{ID_{MS}, PK_{MS}, Z^*_{R_S}\} = D_{K.SS_k}(Y_{MS})$; $Z_{R_S} = H(ID_{MS} \| I_D \| ID_{R_S} \| PK_{AS} \| X_A)$. Upon the Inference of user information, *Ad* executes $Prob2^{EC-DLP}_{K.SS_k\ Ad}$ to recognize the common SS_k of the authorized user. This possibility utilizes the *Reveal* (2) of RoR model to rate the success probabilities and can be defined as $Success2^{EC-DLP}_{K.SS_k\ Ad} = |2_{Pr}\left[Prob2^{EC-DLP}_{K.SS_k\ Ad} = 1\right] - 1|$ to inspect the success rate of adversary *Ad* as $Ad2^{EC-DLP}_{K.SS_k\ Ad}(ID_{MS}, PK_{MS}, Z^*_{R_S}) = Max_{A_d}\left(Success2^{EC-DLP}_{K.SS_k\ Ad}\right)$ separately, where the probability of maximum success rate is measured over A_{dv}. It disclose the RoR model *Reveal* (2). This SUSI scheme is officially known to be safe against A_d particularly to shield the common SS_k of M_S and GW_A, if $Ad2^{EC-DLP}_{K.SS_k\ Ad}(ID_{MS}, PK_{MS}, Z^*_{R_S}) < \varepsilon$, for any insufficiency $\varepsilon > 0$.

Considering the probability $Prob2^{EC-DLP}_{K.SS_k\ Ad}$ that A_{dv} wishes to extract the legitimate information of the user i.e. from the stolen medical device M_D. Upon the successful extraction of the medical data, such as ID_{MS}, ID_{R_S} and SS_k from the GW_A, A_{dv} causes to infer the common SS_k of the M_S and GW_A. Conversely, it is computationally infeasible to compute $Z_{R_S.MS} = H(ID_{MS} \| ID_{R_S} \| PK_{MS.R_S})$. Hence, the proposed SUSI not only achieves a property of user anonymity but also resists the potential attack i.e. the stolen smart device M_D.

5.2 Informal analysis

This analysis shows the security efficiencies of the proposed SUSI. They are as follows:

Property of Proper Mutual Authentication: The proposed SUSI makes the authorized transmission messages, such as $PK_{R_S} = T_{SS_k}(x)\ mod\ q$; $PK_{AS} = T_{R_S}(K_S) = T_{AS}(x)\ mod\ q$; $Y_{MS.R_S} = H(ID_{R_S} \| I_D \| PK_{R_S} \| X_A)$; $Z_{R_S} = H(ID_{R_S} \| Y_{MS.R_S})$; and $Z_{R_S.SS_k} = H(ID_{R_S} \| PK_{R_S} \| PK_A \| X_A)$; and $Z_{R_S} = E_{K.R_S}(ID_{R_S}, I_D, Z_{R_S}, Z_{R_S.SS_k})$ to dispatch $MSG_2 = \{Z_{MS}, PK_A, Z_{R_S}, PK_{R_S}\}$ to GW_A. The specific parameters such as Z_{MS}, PK_A are utilized to prove user legitimacy. Therefore, the proposed SUSI adheres to the property of proper mutual authentication.
Property of Session-Key Agreement: The proposed SUSI uses M_S and R_S to define a key SS_k over the extraction of $Z_{R_S.MS} = H(ID_{MS} \| ID_{R_S} \| PK_{MS.R_S})$; thus this proposed SUSI could generate a valid secret session-key during the execution of the authentication phase. Hence, the proposed SUSI adheres to the property of the session-key agreement.
Property of Known-Key Security: $Z_{R_S.MS} = H(ID_{MS} \| ID_{R_S} \| PK_{MS.R_S})$ is often modified to establish a secure session in a real-time environment. Therefore, A_{dv} cannot

regulate a valid SS_k to interfere with the secret information. Therefore, the proposed SUSI adheres to the property of known-key security.

Property of User-Anonymity: The user identities integrate with $PK_{MS.R_S} = T_{MS}(PK_{AS})T_{MS.R_S}(x)\ mod\ q$; and thus *Ad* cannot infer the sensitive information of the expert without GW_A key. Therefore, the proposed SUSI achieves the security feature of user anonymity.

Irrepressible to Stolen Smart Device Attack: The storage information of M_D does not share the system parameters such as $Z_{R_S.MS} = H(ID_{MS} \| ID_{R_S} \| PK_{MS.R_S})$ for any user. Thus, *Ad* cannot access the database of M_D *and* GW_A to authenticate as a legitimate user. Hence, the proposed SUSI is irrepressible to the stolen smart device attack.

User Friendliness: The proposed SUSI uses M_D to infer his/her own identities, namely ID_{MS}, I_D, and Y_{MS}. Besides, the secret-key of M_D i.e.I_D cannot be altered with proper mutual authentication. Thus, the proposed SUSI offers better user-friendliness to ease the system features.

Irrepressible to Replay Attack: A_{dv} may intervene in the message transmission to break the communication between the authentic clients. Conversely, using ID_{MS} and ID_{R_S}, the real-time entities, namely M_S, and GW_{acces} control the threat activities of A_{dv}. Hence, the proposed SUSI scheme can be irrepressible to replay attack.

Irrepressible to Password-Guessing Attack: Assume that A_{dv} stole the smartcard of a legitimate user to extract the user information of smartcard, such as $\{ G_A, M_A\}$ using side-channel attack [19], where $G_A = H(ID_{MS} \| PWD_{MS} \| I_D) \oplus X_A$; and $M_A = H(ID_{MS} \| I_D \| X_A)$. However, A_{dv} cannot guess a secret key SS_k to compute $PK_{MS.R_S} = T_{MS}(PK_{AS})T_{MS.R_S}(x)\ mod\ q$; $Z_{R_S.MS} = H(ID_{R_S} \| PK_{MS.R_S})$ to validate whether $Z_{R_S.MS}$is not equaled to $Z^*_{R_S.MS}$. Otherwise, M_S aborts the service session; thus A_{dv} cannot verify the legal conformity without the freshness of (ID_{MS}, I_D, X_A). Hence, the proposed SUSI may resist the password-guessing attack.

Irrepressible to Stolen Verifier Table Attack: As the proposed SUSI scheme does not apply the verification table, A_{dv} cannot infer the confidential data of real-time entities. Thus, it can be resilient to a stolen-verifier table attack.

Irrepressible to Privileged-Insider Attack: As M_S always refers the user credentials, such as $\{ID_{MS}, PWD_{MS}, I_D, X_A\}$ to GW_A over an insecure channel, A_{dv} cannot exploit the privileged-insider to infer the user information M_S without random integer x. Thus, the proposed SUSI can be resilient to privileged-insider attack.

Irrepressible to Man-in-the-Middle Attack: The aforesaid analysis proves that the SUSI scheme can offer better authentication between M_S, GW_A, and R_S. Thus, the proposed SUSI can be resilient to the man-in-the-middle attack.

Irrepressible to Key Impersonation Attack: To personate as M_S for GW_A, *Ad* wishes to create a legal message transmission $X^*_{R_S} = G_{R_S} \oplus H(ID_{R_S} \| PWD_{R_S} \| I_D)$; $M^*_{R_S} = H\left(ID_{R_S} \| PWD_{R_S} \| I_D \| X^*_{R_S}\right)$ to check whether M_{R_S} is not equaled to $M^*_{R_S}$. Otherwise, GW_A aborts the service session. However, A_{dv} cannot compute the $MSG_2 = \{Z_{MS}\ , PK_A\ , Z_{R_S}\ , PK_{R_S}\}$ to derive the system parameters. Thus, without extraction of smartcard information, A_{dv} cannot make a valid message transmission. Hence, the proposed SUSI can provide resiliency against key impersonation attack.

Secret-Key Disclosure: Consider that A_{dv} may wish to overhear the transmission message $\{Z_{MS}\ , PK_A\ , Z_{R_S}\ , PK_{R_S}\}$ in the authentication and key update phase. Conversely,

without the determination of $PK_{R_S} = T_{SS_k}(x)\ mod\ q$; $PK_{AS} = T_{R_S}(K_S) = T_{AS}(x)\ mod\ q$; $Y_{MS.R_S} = H(ID_{R_S} \| I_D \| PK_{R_S} \| X_A)$; $Z_{R_S} = H(ID_{R_S} \| Y_{MS.R_S})$; and $Z_{R_S.SS_k} = H(ID_{R_S} \| PK_{R_S} \| PK_A \| X_A)$; and $Z_{R_S} = E_{K.R_S}$ $(ID_{R_S}, I_D, Z_{R_S}, Z_{R_S.SS_k})$, A_{dv} cannot infer secret-key SS_k of M_S to verify whether the expression is equal or not. Hence, the SUSI scheme achieves secret-key disclosure.

Perfect Forward Secrecy: The authentication and key update uses Chebyshev Chaotic-Map assumption to contribute a session key SS_k between $\{Z_{MS}, PK_A, Z_{R_S}, PK_{R_S}\}$ to guarantee perfect secrecy i.e. forward. To launch a secret session key, M_S and GW_A use diverse parameters $\{ID_{R_S}, I_D, Z_{R_S}, Z_{R_S.SS_k}\}$ to create a secure communication i.e. each session, and thus they are dissimilar as compared to the previous values $\left\{ID_{R_S}, ID^*_{MS}, Y^*_{R_S}\right\}$ verifying with $Y_{MS} = H(ID_{MS} \| I_D \| PK_{AS} \| X_A)$ to embrace with transmission delay. Consequently, the previous session-key SS_k of M_S and GW_A cannot disclose to any A_d, whereby a proper session-key cannot be computed to establish a secure between M_S and GW_A without $\{Z_{MS}, PK_A\}$. Hence, the SUSI scheme guarantees perfect forward secrecy between the communication entities such as M_S, R_S and GW_A.

5.2.1 Resilient to sensor node capture attack

In this attack, M_S tries to compromise the confidential information of users to detect the non-compromised sensors and related legitimate users. To evaluate the implications, the deployed sensor node captures the system label as M_S'. Using M_S', A_d captures the sensitive information of M_S that includes SS_{ki}, R_i and its associated former secret session-key SS_k. As the system is not prepared with tamper-resistant, the sensitive information cannot be inferred to share the user information. The proposed SUSI uses secret session-key $PK_{MS.R_S} = T_{MS}(PK_{AS})T_{MS.R_S}(x)\ mod\ q$ to generate and verify with $PK_{AS} = T_{SS_k}(K_S) = T_{MS}(x)\ mod\ q$ to examine whether the computation is equal or not. If the computed values are not identical, then M_S dismisses the session establishment. Moreover, the establishment of secret session-key SS_k can be more discrete and computationally impracticable to gather the system parameters, which is non-invertibility determining one-way hash function. Thus, none of the sensitive information regarding M_S can be exposed to offer the resiliency against sensor-node capture attack.

SP_1: Property of Proper Mutual Authentication; SP_2: Property of Session-Key Agreement; SP_3: Property of Known-Key Security; SP_4: Property of User-Anonymity; SP_5: Resilient to Stolen Smart Card Attack; SP_6: User Friendliness; SP_7: Irrepressible to Replay Attack; SP_8: Irrepressible to Password-Guessing Attack; SP_9: Spirited to Stolen-Verifier Table Attack; SP_{10}: Irrepressible to Privileged-Insider Attack; SP_{10}: Irrepressible to Man-in-the-Middle Attack; SP_{11}: Irrepressible to Key-Impersonation Attack; SP_{12}: Secret key disclosure; SP_{13}:Perfect Forward Secrecy; SP_{14}:Irrepressible to Sensor Node Capture Attack; and SP_{15}: Efficient Secret-Key Exchange.

5.2.2 Efficient secret-key exchange

The existing schemes [12, 26, 31, 37] ought to have a lack of input authentication, where a secret key update phase does not tolerate the legal use to login to the system server using a smart device. On the other hand, the legitimate user may not gain the server access, when he/she incorrectly passes the secret session-key during the key update phase. Since the proposed

SUSI declares the new value to verify with the previous one, it may not allow any fabricated values in the key update phase. Hence, the proposed SUSI achieves better secret-key exchange as compared to other existing schemes [12, 26, 31, 37].

Table 3 demonstrates the comparison of security efficiencies for proposed SUSI and existing schemes [12, 26, 31, 37]. From Table 3, it is observed that the SUSI scheme delivers a more competent and operative solution to preserve the entities, such as M_d, S_N and GW_{access} close to various possible attacks illustrated in Table 3. Moreover, the proposed SUSI scheme proves better security efficiencies than other existing schemes [12, 26, 31, 37].

5.3 Performance comparison

Table 4 shows the assessment of performance analysis for proposed SUSI and existing schemes [12, 26, 31, 37]. As referred in [9], the time consumption of one-way hash function T_H, signature T_S and symmetric key encryption/decryption $T_{E/D}$ are considered as 0.0004 s, 0.1303 s, and 0.3317 s respectively. The proposed SUSI scheme considers the above values to analyze the communication overhead of the login and authentication phase. From Table 1, the transmission length of real-time entities such as M_d, R_S and GW_A is defined as 160 *bits*. The comparative analysis is as follows:

1. The proposed SUSI consumes less time during the system registration phase than other existing schemes [12, 26, 31, 37].
2. At GW_A, the proposed SUSI demonstrates less time consumption as compared to other authentication schemes [12, 26, 31, 37].
3. At M_S, the proposed SUSI scheme records less time consumption to improve the transmission efficiency and data analysis as compared to other schemes [12, 26, 31, 37].
4. At R_S, the proposed SUSI scheme consumes less execution time than Li et al. [26], however, it consumes more execution time than other authentication schemes [12, 31, 37].
5. The communication cost of proposed SUSI scheme is recorded into ⟨1280 *bits*⟩, which is comparatively more than Deebak et al. [12] but less than the other existing schemes [26, 31, 37].

Table 3 Comparison of Security Efficiencies

Security Properties	Li et al. [26]	Deebak et al. [12]	Madhusudhan et al. [31]	Srinivas et al [37]	Proposed SUSI
SP_1	√	√	√	√	√
SP_2	×	√	×	√	√
SP_3	×	×	×	√	√
SP_4	×	√	√	√	√
SP_5	×	√	×	√	√
SP_6	×	√	√	√	√
SP_7	√	√	√	√	√
SP_8	×	×	√	√	√
SP_9	×	√	×	×	√
SP_{10}	×	×	√	×	√
SP_{11}	×	×	√	√	√
SP_{12}	×	×	×	×	√
SP_{13}	√	×	√	×	√
SP_{14}	×	√	×	×	√
SP_{15}	×	×	√	√	√

Table 4 Performance Comparison of Proposed SUSI and Existing Authentication Schemes

Performance Parameters		Li et al. [26]	Deebak et al. [12]	Madhusudhan et al. [31]	Srinivas et al [37]	Proposed SUSI
Storage Space in Smart Device (M_D)		832	704	832	640	520
System Login and Authentication Phase (ms)	(M_S)	$10T_H + 4T_{E/D} + 2T_S$	$6T_H + 1T_{E/D}$	$3T_H + 2T_{E/D}$	$8T_H + 2T_{E/D}$	$3T_H + 1T_{E/D}$
	(GW_A)	$1T_S + 3T_{E/D} + 11T_H$	$9T_H + 2T_{E/D}$	$1T_H + 2T_{E/D}$	$4T_H + 1T_{E/D}$	$8T_H + 1T_{E/D}$
	(R_S)	$4T_S + 8T_{E/D} + 16T_H$	$7T_H$	$2T_H + 2T_{E/D}$	$4T_H + 2T_{E/D}$	$6T_H + 2T_{E/D}$
	Computation Cost (s)	5.888	1.004	1.993	1.663	1.334
Communication Cost (bits)		4192	1216	2000	1504	1280
Formal Analysis		No	No	Yes	Yes	Yes
Message Rounds		4	4	5	4	4

6. The proposed SUSI previously demonstrates its safety measures in both formal and informal analysis; and thus the major weaknesses of existing schemes can be dealt with successfully [12, 26, 31, 37].
7. The computation of proposed SUSI records less calculation cost with other schemes [12, 26, 31, 37], as it operates with minimum cost to establish a secure message transmission between the real-time entities.
8. While probing the operation cost of the login and authentication phase, most of the authentication schemes report fewer transmission rounds between the communication entities as compared to Madhusudhan et al. [31]. Most importantly, the SUSI scheme is verified to be well secure over the potential threats depicted in Table 2 in comparison with other schemes [12, 26, 31, 37].

6 Practical analysis

This section demonstrates the practical examination using NS3 to examine the communication metrics such as Transmission Delay $\langle T_D \rangle$ and Throughput Rate $\langle T_R \rangle$. To realize the network simulation, an extensive NS3 version i.e. NS-3.28 has been installed in Ubuntu 14.04 LTS. Table 5 defines the important simulation parameters that include network coverage i.e. 100 ×

Table 5 Simulation Parameters Used

Network Parameter	Description
Operating System	Ubuntu 14.04 LTS
Network Simulator	NS-3.28
Number of Communication Nodes	⟨2, 6, 2⟩
Number of Medical Sensor Nodes	⟨160⟩
Number of Remote Server	⟨3⟩
Packet Size	⟨144 *bits*⟩,⟨80 *bits*⟩,⟨64 *bits*⟩
Gateway Location	$\langle 50 \times 25\ m^2 \rangle$
Traffic Type	⟨*TCP*/*UDP*⟩
Interval Time	0.5 *s*
Mobility Speed	⟨≈2 *to* 50 *m*/*s*⟩
Initialization of a Node Energy	⟨≈3600 *J*⟩
Transmission Power	⟨28 *dBm*⟩
Voltage supplied	⟨3 *V*⟩

100 m^2 to examine transmission scenario between M_S, GW_A, and R_S with a node distance of 25 m to 50 m, studied in [12]. A wireless standard i.e. *IEEE* 802.15.4 is chosen as a media access control (*MAC*) to simulate the network ≈1800 *sec* i.e. 30 *min*. To realize the transmission scenario, an optimized link-state routing protocol ⟨*OLSR*⟩ is preferred that provides dynamic routing to uphold the importance of distributed routing among the communication entities such as M_S, GW_A, and R_S. (Table 5)

To investigate the communication metrics, M_S nodes are distributed in rectangular form. In the simulation, ⟨20⟩ sensors are administered in a row that may subsequently incur more number of rows in the execution scenario, constructively not more than ⟨8⟩ rows. To investigate the network, two gateway nodes GW_A, six medical sensors M_S and 2 remote servers R_S are deployed. This is a note that GW_A is regularly inspected to examine the transmission scenario, which includes four transmission messages such as $MSG_1 = \{Z_{MS}, PK_A\}$, $MSG_2 = \{Z_{MS}, PK_A, Z_{R_S}, PK_{R_S}\}$, $MSG_3 = \{Z_{MS}, Z_{R_S}\}$, and $MSG_4 = \{Y_{MS}, Z_{R_S.MS}\}$. The above transmission messages are periodically invoked with the given packet size to examine the quality metrics such as $\langle T_D \rangle$, and $\langle T_R \rangle$. Each smart device M_D initiates the message transmission for the interval of 0.5 *s*.

6.1 Analysis 1: Transmission delay $\langle T_D \rangle$

T_D is generally defined as the expected time-taken by the data packets to the sink node from the source node. The overall computation is as follows: $T_D = \sum_{i=1}^{N_{DP}} \frac{(DP_i^R - DP_i^S)}{N_{DP}}$, where N_{DP} is the number of transmitted data packets; $\langle DP_i^R, DP_i^S \rangle$ are the data packets initiated by the sender and receiver for the given network scenario. From Fig. 3, it is found that the proposed SUSI reports less transmission delay than other existing schemes [26, 31, 37] except for Deebak et al. [12]. The average transmission delays of proposed SUSI and other existing schemes are recorded as follows:0.216 *s*, 0.146 *s*, 0.174 *s*, 0.167 *s*, and 0.153 *s* respectively. From the simulation, it is also noted that the transmission delay soars up when the number of

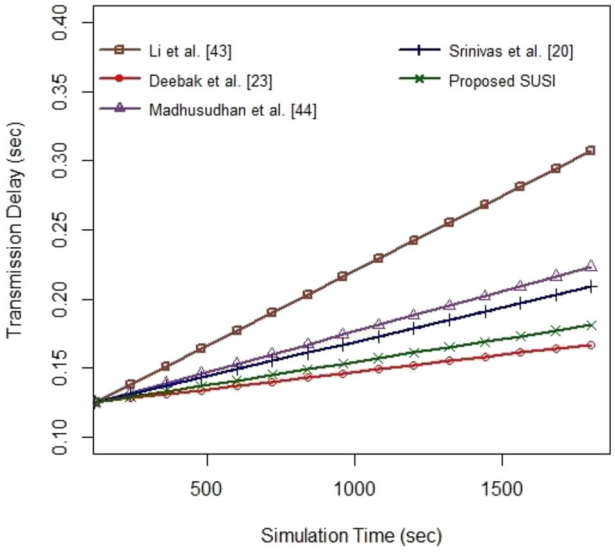

Fig. 3 Transmission Delay (*sec*)

packet transmission increases proportionally by the communication nodes. However, the proposed SUSI keeps the delay within the restricted limit in the use of less message rounds between the communication entities such as M_S, GW_A, and R_S than the other existing schemes [26, 31, 37] excluding Deebak et al. [12].

6.2 Analysis 2: Throughput rate $\langle T_R \rangle$

T_R is generally defined as the number of successfully transmitted bits per execution time. The overall computation can be expressed as follows: $\langle T_R \rangle = \frac{(TN_P \times |P_K|)}{T_T}$, where TN_P is the total number of data packets received successfully, P_K is the transmission packet; and T_T is the total transmission time. From Fig. 4, it is noticed that the proposed SUSI achieves a better throughput rate than other existing schemes [26, 31, 37] excluding Deebak et al. [12]. The simulation study shows that the execution time was considered to analyze the successful transmission packets i.e. for proposed SUSI and other authentication schemes [12, 26, 31, 37]. The average successful transmission bits of proposed SUSI and other existing schemes are recorded as follows:675 *bits*, 850 *bits*, 1025 *bits*, 640 *bits*, and 1165 *bits*respectively. This is to note that the proposed SUSI has a slight deviation at 560 *s* to 960 *s* due to more number of transmission packets among the communication nodes.

6.3 Analysis 3: Packet delivery ratio $\langle P_{DR} \rangle$

P_{DR} investigates the strength of the transmission link in terms of reliability to evaluate the delivery ratio of the transmitted packets. Since the evaluation result fixes the link reliability ≈90%, the simulation is not performing packet retransmission to validate the proof of delivery ratio.

Figure 5 shows the packet delivery ratio ⟨%⟩ versus the simulation time ⟨*sec*⟩ with link reliability ≈90%. Since the proposed SUSI handles the random identities efficiently, it

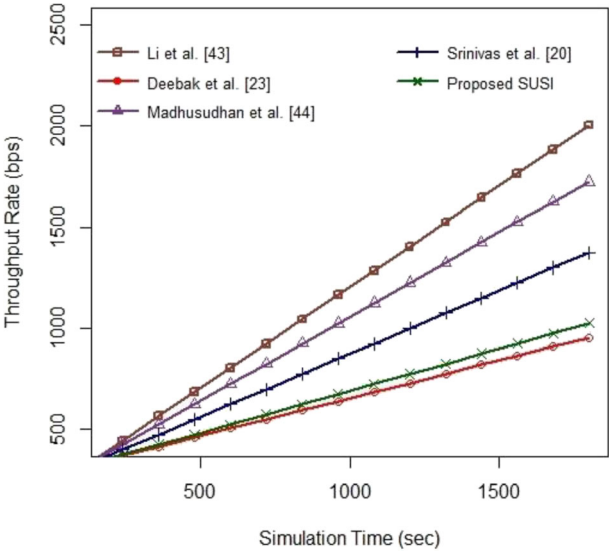

Fig. 4 Throughput Rate (*bps*)

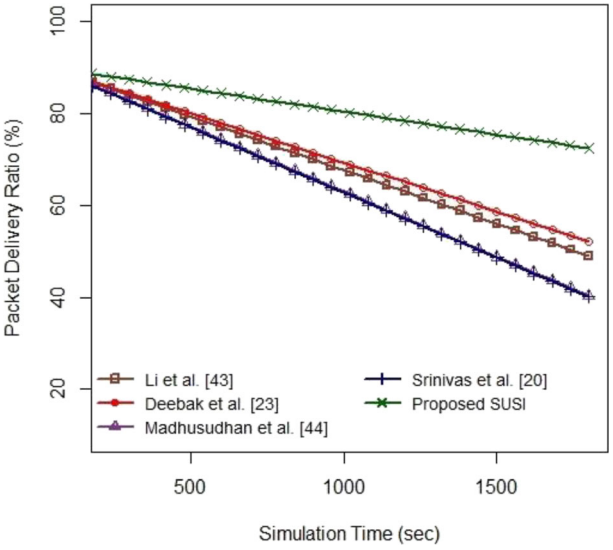

Fig. 5 Packet Delivery Ratio ⟨%⟩

guarantees the data freshness to authorize the data from the remote server access. Moreover, the proposed SUSI utilizes fewer computation operators to process the data forwarding; thereby the energy consumption of the node is minimized. However, the other existing schemes neglect the important factors of the transmission link resulting in packet loss. Most importantly, the proposed SUSI evaluates transmission messages with limited message rounds to eliminate the traffic congestion and to improve the delivery ratio of the transmitted packets. The examination result reveals that the proposed SUSI achieves a better delivery ratio $\approx of$ 11.8 % , 10.25 % , 16.15 % , and 16.35% than other existing schemes [12, 26, 31, 37] to improve the routing efficiencies of the network.

7 Conclusions

The major divergence among the nations is the protection of citizen data to meet the global constraint of user privacy. It has limited data access for the healthcare authorities and researchers, which deal with a large amount of medical data to analyze the challenges of privacy protection. Since the data are immeasurable to the medical experts, most of the researchers may work harder on confidential data of the patient to regulate the risks of non-compliance. Therefore, in this paper, a Single User Sign-In (SUSI) has been proposed for RM-PoC using WMSN. The proposed SUSI utilized remote user to strongly exchange a session key to any available sensor node that employs a privacy-preservation strategy to achieve a proper mutual authentication between the communication entities. From the security analysis, the proposed SUSI scheme proves that it cannot only achieve the security properties of AKA protocol, such as proper mutual authentication, secret session-key agreement, etc., but also be resilient to a stolen smart device, privileged-insider and password-guessing attack. As the proposed SUSI satisfies the security goals of WMSN, it can be well suited for the healthcare application systems using WMSN. The proposed SUSI uses an extended Chebyshev Chaotic-Map to preserve user anonymity to prevent information leakage. Using security and performance analysis, the proposed SISI claims the improved efficiencies in comparison with other existing

schemes [12, 26, 31, 37]. Moreover, the simulation results show that the computation of proposed SUSI has less transmission costs to operate the message transmission between the real-time entities to prove its better efficiencies in terms of transmission delay, throughput rate, and packet delivery ratio. In the future, a possible remote registration will be incorporated to investigate the practical and computation difficulties.

References

1. Al-Turjman F, Ever YK, Ever E, Nguyen HX, David DB (2017) Seamless key agreement framework for mobile-sink in IoT based cloud-centric secured public safety sensor networks. IEEE Access 5: 24617–24631
2. Amin R, Maitra T, Giri D, Srivastava PD (2017) Cryptanalysis and improvement of an RSA based remote user authentication scheme using smart card. Wirel Pers Commun 96:4629–4659
3. Awasthi AK, Srivastava K, Mittal RC (2011) An improved timestamp-based remote user authentication scheme. Comput Electr Eng 37(6):869–874
4. Chandrakar P (2019) A secure remote user authentication protocol for healthcare monitoring using wireless medical sensor networks. Int J Ambient Comput Intell (IJACI) 10(1):96–116
5. Chaudhary RRK, Singh A, Chatterjee K (2020) An enhanced authentication scheme for internet of things based E-healthcare system. J Comput Theor Nanosci 17(1):246–253
6. Chen TH, Shih WK (2010) A robust mutual authentication protocol for wireless sensor networks. ETRI J 32(5):704–712
7. Das AK, Bruhadeshwar B (2013) An improved and effective secure password based authentication and key agreement scheme using smart cards for the telecare medicine information system. J Med Syst 37(5):1–17
8. David DB, Rajappa M, Karupuswamy T, Iyer SP (2015) A dynamic-identity based multimedia server client authentication scheme for tele-care multimedia medical information system. Wirel Pers Commun 85(1): 241–261
9. Deebak BD (2017) Mutual Authentication Scheme for Multimedia Medical Information System. Multimedia Tools Appl 76(8):10741–10759 (IF-1.53)
10. Deebak BD, Muthaiah R, Thenmozhi K, Swaminathan P (2015) Evaluating three party authentication and key agreement protocols using IP multimedia server–client systems. Wirel Pers Commun 81(1):77–99
11. Deebak BD, Muthaiah R, Thenmozhi K, Swaminathan PI (2016) Analyzing three-party authentication and key agreement protocol for real time IP multimedia server–client systems. Multimed Tools Appl 75(10): 5795–5817
12. Deebak BD, Al-Turjman F, Aloqaily M, Alfandi O (2019) An authentic-based privacy preservation protocol for smart e-healthcare systems in IoT. IEEE Access 7:135632–135649
13. Dharminder D, Gupta P (2019) Security analysis and application of Chebyshev chaotic map in the authentication protocols. Int J Comput Appl. 2019:1–9
14. Farasha MS, Turkanovic M, Kumaric S, Hölbl M (2016) An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment. AdHoc Networks 36:152–176
15. Franks J, Hallam-Baker P, Hostetler J, Lawrence S, Leach P, Luotonen A, Stewart L (1999) HTTP authentication: basic and digest access authentication. Network Working Group 1999:78
16. Gope P, Das AK, Kumar N, Cheng Y (2019) Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks. IEEE Trans Ind Informa 15(9):4957–4968
17. Gunasinghe H, Bertino E (2017) PrivBioMTAuth: privacy preserving biometrics-based and user centric protocol for user authentication from mobile phones. IEEE Trans Inf Forensics Secur 13(4):1042–1057
18. Hu P, Ning H, Qiu T, Song H, Wang Y, Yao X (2017) Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things. IEEE Internet Things J 4(5):1143–1155
19. Huang X, Xiang Y, Chonka A, Zhou J, Deng RH (2011) A generic framework for three-factor authentication: preserving security and privacy in distributed systems. IEEE Trans Parallel Distrib Syst 22(8):1390–1397
20. ICS 35.040.50, Information technology—Smart transducer interface for sensors and actuators — Part 7: Transducer to radio frequency identification(RFID) systems communication protocols and Transducer Electronic Data Sheet (TEDS) formats (2011) ISO/IEC/IEEE Std 21451–7, pp.1–82

21. Jiang Q, Khan MK, Lu X, Ma J, He D (2016) A privacy preserving three-factor authentication protocol for e-health clouds. J Supercomput 72(10):3826–3849
22. Kumari A, Yahya Abbasi M, Kumar V, Khan AA (2019) A secure user authentication protocol using elliptic curve cryptography. J Discret Math Sci Cryptogr 22(4):521–530
23. Lamport L (1981) Password authentication with insecure communication. Commun ACM 24(11):770–772
24. Le XH, Khalid M, Sankar R, Lee S (2011) An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare. J Netw 6(3):355–364
25. Li X, Niu J, Kumari S, Liao J, Liang W, Khan MK (2015) A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity. Secur Commun Netw 9(15): 2643–2655
26. Li CT, Shih DH, Wang CC (2018) Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems. Comput Methods Prog Biomed 157:191–203
27. Li X, Peng J, Obaidat MS, Wu F, Khan MK, Chen C (2019) A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems. IEEE Syst J 14(1):39–50
28. Li J, Zhang N, Ni J, Chen J, Du R (2020) Secure and lightweight authentication with key agreement for smart wearable systems. IEEE Int Things J 7(8):7334–7344
29. Liu H, Ning H, Xiong Q, Yang LT (2014) Shared authority based privacy-preserving authentication protocol in cloud computing. IEEE Trans Parallel Distrib Syst 26(1):241–251
30. Liu H, Yao X, Yang T, Ning H (2018) Cooperative privacy preservation for wearable devices in hybrid computing-based smart health. IEEE Internet Things J 6(2):1352–1362
31. Madhusudhan R, Shashidhara R (2020) Mobile user authentication protocol with privacy preserving for roaming service in GLOMONET. Peer-to-Peer Netw Appl 13(1):82–103
32. Mo J, Hu Z, Lin Y (2020) Cryptanalysis and security improvement of two authentication schemes for healthcare systems using wireless medical sensor networks. Secur Commun Networks 2020:*1–11*
33. Odelu V, Das AK, Goswami A (2015) An efficient ECC-based privacy-preserving client authentication protocol with key agreement using smart card. J Inf Sec Appl 2 1:1–1 9
34. Oueida S, Kotb Y, Aloqaily M, Jararweh Y, Baker T (2018) An edge computing based smart healthcare framework for resource management. Sensors 18(12):4307
35. Oueida S, Aloqaily M, Ionescu S (2019) A smart healthcare reward model for resource allocation in smart city. Multimed Tools Appl 78(17):24573–24594
36. Shen JJ, Lin CW, Hwang MS (2003) Security enhancement for the timestamp-based password authentication scheme using smart cards. Comput Secur 22(7):591–595
37. Srinivas J, Mishra D, Mukhopadhyay S (2017) A mutual authentication framework for wireless medical sensor networks. J Med Syst 41(5):80–99
38. Turkanovic M, Brumen B, Hölbl M (2014) A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion. Ad Hoc Netw 20:96–112
39. Wang L (2014) Analysis and enhancement of a password authentication and update scheme based on elliptic curve cryptography. J Appl Math 247836:1–11
40. Wang F, Xu G, Xu G (2019) A provably secure anonymous biometrics-based authentication scheme for wireless sensor networks using chaotic map. IEEE Access 7:101596–101608
41. Wang F, Xu G, Xu G, Wang Y, Peng J (2020) A robust IoT-based three-factor authentication scheme for cloud computing resistant to session key exposure wireless communications and mobile computing. Wirel Commun Mob Com 3805058:1–15
42. Wu F, Xu L (2013) Security analysis and improvement of a privacy authentication scheme for telecare medical information systems. J Med Syst 37(4):1–9
43. Yang G, Wong DS, Wang H, Deng X (2008) Two-factor mutual authentication based on smart cards and passwords. J Comput Syst Sci 74(7):1160–1172
44. Yu Y, Au MH, Ateniese G, Huang X, Susilo W, Dai Y, Min G (2016) Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. IEEE Trans Inf Forensics Sec 12(4):767–778
45. Zhang L (2008) Cryptanalysis of the public key encryption based on multiple chaotic systems. Chaos, Solitons Fractals 37(3):669–674
46. Zhu H, Hao X, Liu H (2015) An effcient authenticated key agreement protocol based on chaotic maps with privacy protection using smart card. J Inf Hiding Multimedia Signal Process 6(3):500–510

Affiliations

B. D. Deebak[1] · Fadi Al-Turjman[2] · Anand Nayyar[3,4]

✉ B. D. Deebak
deebakbd@gmail.com

[1] School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, India

[2] Research Center for AI and IoT, Near East University, Nicosia, Mersin 10, Turkey

[3] Graduate School, Duy Tan University, Da Nang 550000, Viet Nam

[4] Faculty of Information Technology, Duy Tan University, Da Nang 550000, Viet Nam