Complex & Intelligent Systems
https://doi.org/10.1007/s40747-020-00231-7

ORIGINAL ARTICLE

Secure-user sign-in authentication for IoT-based eHealth systems

B. D. Deebak[1] · Fadi Al-Turjman[2]

Received: 4 August 2020 / Accepted: 3 November 2020

Abstract

Sustainable Computing has advanced the technological evolution of the Internet and information-based communication technology. It is nowadays emerging in the form of the Cloud of Medical Things (CoMT) to develop smart healthcare systems. The academic community has lately made great strides for the development of security for the CoMT based application systems, such as e-healthcare systems, industrial automation systems, military surveillance systems, and so on. To the architecture of CoMT based Smart Environment, Chebyshev Chaotic-Map based single-user sign-in (S-USI) is found as a significant security-control mechanism. To ensure the fidelity, the S-USI assigns a unary-token to the legal users to access the various services, provided by a service provider over an IP-enabled distributed networks. Numerous authentication mechanisms have been presented for the cloud-based distributed networks. However, most of the schemes are still persuasible to security threats, such as user-anonymity, privileged-insider, mutual authentication, and replay type of attacks. This paper applies a sensor/sensor-tag based smart healthcare environment that uses S-USI to provide security and privacy. To strengthen the authentication process, a robust secure based S-USI mechanism and a well-formed coexistence protocol proof for pervasive services in the cloud are proposed. Using the formal security analysis, the prominence of the proposed strategies is proven to show the security efficiency of proposed S-USI. From the formal verification, the comparison results demonstrate that the proposed S-USI consumes less computation overhead; and thus it can be more suitable for the telecare medical information systems.

Keywords Pervasive services · Cloud of Medical Things · Chebyshev Chaotic-Map · Single user sign-in · Security · Privacy · Distributed network · Telecare medical information systems

Abbreviations

CoMT	Cloud of Medical Things
S-USI	Single-user sign-in
TMIS	Telecare medical information systems
IoT	Internet of Things
ICT	Information and communication technology
AKA	Authentication and key agreement
PHI	Protected health information
WAP	Wireless application protocol
XaaS	Everything as a service
QoS	Quality of service
IoMT	Internet of Medical Things
IoUT	Internet of Underwater Things
IoNT	Internet of Nano Things
WMSN	Wireless medical sensor networks
NIST	National Institute of Standards and Technology
IaaS	Infrastructure as a service
PaaS	Platform as a service
SaaS	Software as a service
WSN	Wireless sensor networks
DoS	Denial of service

Introduction

Of late, smart sustainable cities have been engaged in the recreation activities of the individual. It is nowadays converging the technological aspects of IoT and its associated big data applications to develop intelligent computing systems [1]. This is underlying as the technological core in the construction of numerous transformations. To exhibit the data characteristics, the state of the attributes such as monitoring, collecting, processing, and analyzing are explicitly

✉ B. D. Deebak
deebak.bd@vit.ac.in

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

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

Published online: 03 January 2021

regenerated that controls the environmental condition of smart cities. Various intelligent systems such as energy, automation, infrastructure, and transport utilize the core developments of IoT and big data applications to build sustainable environs. Smart sustainable cities typically meet the standard requirements of pervasive and mobile intelligence [2]. It uses distributed computing to establish communication between the IoT objects that offer informational services to the urbanites [3]. A technological change characterizes the significance of disruptive technologies that embed the techniques of ICT to address the complexities of techno-urban systems.

The urban domains may apply ICT technologies to implicate the environment features [1]. The technological evolution emerges the ICT visions to develop sustainable computing systems including infrastructure, facilities, services, resources, design, etc. The pervasive intelligence may integrate these important features to manage environmental issues [2]. A computing paradigm may use big data analytics to realize the key factors of novel applications that stimulate the development of sustainable systems. In the past, the ICT has dramatically changed for the maximization of service connectivity that closely associates with the cloud computing systems as a platform to enable environmental services. Most of the information services integrate PaaS to operate computing services through centralized systems. According to Statista, the cloud market is expected to grow $163billion in 2021 that increases the connectivity of IoT devices to improve communication efficiency [4].

The convergence technologies such as augmented reality, autonomous driving, and smart cities are continuously being transformed to meet the standard requirements such as communication speed, bandwidth, and low-latency. It may synergize with IoT technology to improve service efficiency, which unifies the network structures to manage the high-level services. However, it has three major perspectives to address security issues: (1) drive the network traffic to examine the device connectivity; (2) increase the service connection over a cloud platform; (3) integrate the heterogeneous network to identify security issues. In the advancement of cloud computing technologies, the cloud assistive electronic healthcare systems are growing rapidly for remote e-healthcare services. Various security solutions with different application aspects [5, 6] shave been proposed for cloud-computing systems that are very much suitable to build a secure e-healthcare system.

A popular domain, known as TMIS [7, 8] has been one of the more suitable applications for remote electronic healthcare systems. However, the TMIS application can be emerged with a cloud assistive cognitive aware e-healthcare system to facilitate the medical diagnosis and the storage of healthcare records. The medical entities such as medi-expert, patient, and server-database are preferred to transmit the medi-data over insecure public networks. The data fabrication may lead to severe hazards; and thus it should be kept secret to provide patient's privacy and convenient access. Therefore, a secure data transmission in TMIS has become a hot issue for wireless channel access. For the protection of information access over public networks [9], a method such as AKA has been chosen i.e. for the communication processes [10, 11].

Moreover, a secret password and a data storage like a smartcard or smart device comprising of secret-data possessed by the authentic-user is applied in the remote user authentication system. This communication device is distributed as a trustworthy server that wants the user to submit his/her information such as patient identity and string preprocessor to the registration server. As the network-based application system exists with various malicious activities, they may even forge or overhear the data transmission to disrupt the legal communication access. Most dangerous attacks such as server spoofing, key impersonation, and offline guessing have been addressed by various existing authentication schemes [12–14]. In urban cities, hospital management systems are growing rapidly to offer emergency services that meet the medical demands of the common people.

CoMT uses distributed networks that provide legal user access to disseminate the private user information, whereby less power computation is achieved with the available devices [15]. In general, the public or private service provider is nominated to distribute the authentic accesses, which deliver the application services to gain the network resources more efficiently. Generally speaking, the application should obtain a reliable transmission region to gain network access of the service provider. It has different users with distinct identities/secret key pairs to gain the exclusive rights of resource usage [16]. Figure 1 shows the electronic healthcare architecture using a CoMT. The biological sensors estimate the physiological conditions of the patient to feed the patients' information i.e. to the smart computing devices whereby the data are transmitted through the knowledge of healthcare service providers over public Internet access.

Upon the information access, the data storage server accommodates the PHI of patients that gains the user access to grant the implementation policy governed by the policy certification server. After the successful authentication, the authentication server shows the data blocks comprising of patient info, medi-expert, authentic server, and TMIS. In electronic healthcare systems, the patients acquire the PHI to monitor the patient's health condition that is very much useful to provide a medical prescription. In an emergency, a smart ambulance service can be initiated to offer timely user access to extend medi-service to the casualty before they reach the hospital. Importantly, the research and

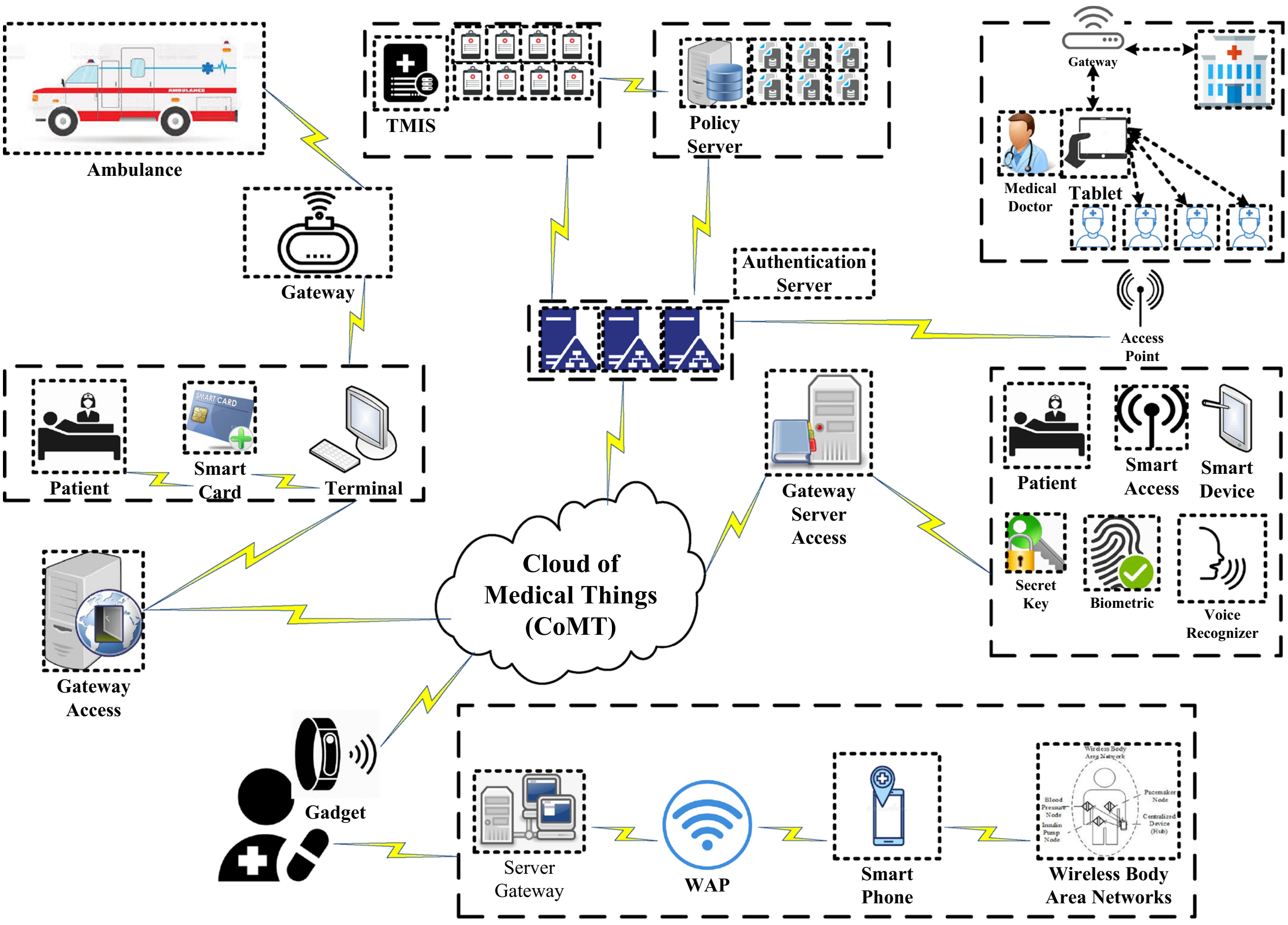


Fig. 1 Electronic healthcare architecture using cloud of things

development process intensively analyzes the sensor input/output to envisage the critical condition of the patient.

Various key authentication mechanisms have been presented using the two-factor and three-factor authentication protocol that was introduced in [17]. As the Lamport scheme was very generic to access the remote-server i.e. user name and password, it could not provide user privacy and anonymity to address the major concern of the electronic healthcare system. In 1990, Hwang has initially presented the two-factor authentication, whereas, in the early 21st century, the three-factor authentication and key agreement protocol was proposed. Commonly, the electronic healthcare system initiates the system registration phase to gain remote user access with TMIS. Upon successful registration, the user gains the authentication to grant access to TMIS. Generally speaking, the one-factor authentication was much easier to remember as the user tries to provide the user name and password to obtain the desirable authentication process, whereas the two-factor additionally incorporates the entities known as smartcard that could subdue the user comforts. In the three-factor, the user may involve biometric information in addition to the real-time entities namely smartcard, username, and password to process the service authentication.

The authentication process comprises of four system phases that are as follows:

System registration In registration, the user wishes to provide the credentials with TMIS such as personal identities and information. Upon which they may choose a secret password at the registration or later phase. Moreover, it is subjected to alter their secret password after the successful login.

System login and authentication In login and authentication, the user may gain the service access provided by TMIS upon the verification of user credentials.

Session key update This phase is employed to change the user credentials secretly that reduces the attack vulnerabilities owing to the use of identical secret-key.

Key revocation This phase is employed to revoke the user credentials in case of key compromising.

Though the user terminal or device has a valid secret key to gain the medical services of the network, the massive data access may be prone to severe network risk, communication, and storage overhead. Therefore, the recent authentication mechanisms have constructed a strategy of control access using advanced mobile computing systems. Of late, three-party authentication and key agreement schemes have been proposed for WMSNs using a smartcard [18, 19]. The design objectives of their system were to provide an effective security mechanism in WSNs. Though their schemes cannot be practically implemented to exercise a time-synchronization mechanism. Moreover, it can be preferred to annul the clock time regulation between the communication parties. Therefore, the S-USI is proposed, which applies a mechanism of unary control access to monitor the device activities. This proposed mechanism annuls the clock synchronization problem for pervasive services in the cloud. In addition, a smart S-USI mechanism demands the multimedia medical sensor network to sense, monitor, and analyze the patient's information effectively. The major contributions are as follows:

1. Design a robust secure based S-USI mechanism to annul the clock synchronization in a pervasive computing environment.
2. Apply unary control access to infer the activities of the medical sensor networks that provide service-level agreement to mitigate the cost of the communication device.
3. Perform the formal analysis using AKE session-key security and BAN logic to prove the security efficiencies of the proposed S-USI including session-key protection.
4. Analyze the key factors including computation, communication, and storage to guarantee the system features of the computing paradigms.

The rest of the sections are devised follows: "Research background" discusses related authentication schemes, important notation, assumption of Chebyshev chaotic maps, and the attacker model. "Proposed single user sign-in (S-USI) mechanism" presents a proposed S-USI mechanism that is completely based on the extended Chebyshev chaotic-map. "Security analysis" demonstrates the security analysis of the proposed S-USI mechanism using AKE session-key security and BAN logic. "Discussions" discusses the challenges of user authentication protocols. "Conclusion" concludes the research work.

Research background

This section summarizes the related authentication schemes, important notation, assumption of Chebyshev chaotic maps, and attacker model.

Emerging computing paradigm

The computing paradigm becomes more prevalent to standardize the parallel and distributed system that consists of visualized and interconnected devices to offer unified computing resources [20]. It is provisionally based on service-level agreement to negotiate the resources between the consumers and the service providers. Moreover, it has an intelligent model to enable on-demand network access to share a pool of computing resources. It can be provisionally released to manage the resources with minimal efforts or over service provider interaction [21]. Senyo et al. [22] outlined cloud computing as 'IT infrastructure, application service, and resource delivery coexist to meet the demands of the individual or organization over a dedicated Internet platform'. The definition can hardly integrate the feature characteristics to consider the subsets of visualized computing systems. Hence, the NIST asserts three different service models such as IaaS, PaaS, and SaaS to claim a variant of security as a service. It is specifically considered for the development of IT infrastructure and application services. It has new phenomena as anything as a service or XaaS to offer minimal interaction with service providers including a pay-per-use basis.

In spite of its pervasiveness, emerging technologies are still active in the area of cloud computing. It has technological convergence to cover the performance aspects such as service automation, service provision, dynamic workloads, resource sharing, multiple tenancies, energy management, virtual machine migration, etc. [23]. The other direction includes benchmark evaluation, reliability, efficiency, scalability, and elasticity to meet the decision supports of cloud computing services. In addition, it has some computing factors namely trustworthiness, readiness, security, privacy, cost, pricing, etc. to adopt the management benefits [24]. Of late, it has emerged several research directions including e-government, e-learning, eHealth, big-data, data processing, and analytics for the prevalence of mobile computing platforms. It refers to smart devices, which are portable, programmable, and scalable to achieve convenient access. These device features are considered as an essential part to meet the service demands including voice communication, data storage, and social interactivity. It is nowadays converging in some specific domains such as m-Health, m-Learning, m-Commerce, etc. that typically focus on drug discovery, online learning, and commercial transaction. The smart device integrates the sensor packages and hardware components to extract the context features. As a result, several context-aware applications have been developed for significant services such as location tracking, proximity measurement, service rating, prediction, etc. [25].

The computing paradigms including mobile, cloud, and IoT emerge as the future dominants to consider the pairwise intersections. It has several areas such as mobile edge computing, web of things, mobile cloud, semantic web of things, cloudlet computing, etc. to explore the property of seamless connectivity [26]. Figure 2 shows the intersection areas of emerging computing paradigms. The convergence technologies such as IoT, cloud, and mobile envision to obtain the human-centric data that differentiates the evolution of pervasive and ubiquitous computing to provide seamless connectivity and human interaction. The interconnected things use sensors and actuators to integrate low-power wireless devices such as IoMT, IoNT, and IoUT to develop an IoT-enabled platform. The futuristic IoT-based healthcare scenarios include remote monitoring, service availability, accessibility, drug management, to offer seamless connectivity via wireless technologies such as Bluetooth, Zigbee, Infrared, and 4G/5G. Since the eHealth data is open to access in the public network, it is highly demanding a secure cryptography protocol to achieve distinct features such as immutable, timestamped, and decentralized. In eHealth, various sensory technologies are integrated to provide an effective solution including end-to-end connectivity, data analysis, tracking, medical alerts, and assistance.

The IoT-based computing systems leverage the automation process, workflow management, and risk deduction to save human life. However, it has several open challenges such as device integration, security, privacy, and data overloading to degrade the efficiency of the healthcare systems. To address the issues, computing paradigms such as fog, edge, cloudlet, and crowdsensing are preferred. It can apply the cryptography protocol to analyze the cloud data via dedicated gateways that address the security challenges among the mobile devices and hubs. The major significances are as follows:

1. Edge computing is an avenue to resolve the issues of low latency and user proximity to the existing IoT users.
2. The other computing solves the research perspectives including location-aware, user-centric, and provisional access to eHealth domains.
3. Scalability is a specific feature to improve the efficiency of the sensory system that integrates the sensor platform to meet the requirements of distributed networks.
4. QoS is more significant to improve the service efficiency of the healthcare systems.

Table 1 summarises the key challenges of the existing works. The personalized healthcare system has some major significances such as reliability, interoperability, and scalability to meet the challenges of IoT [27] that emerges the application requirements of eHealth. Balli et al. [28] reviewed the service features of the electronic devices that materialize the demands of the system design. Chandhuri et al. [29] studied different types of healthcare data and management techniques. Suguna et al. [30] discussed several diagnostic mechanisms under the strategies of IoT protection. Gandhi et al. [31] introduced healthcare intelligence to examine the process of IoT framework. Khan et al. [32] studied various healthcare mechanisms to analyze security

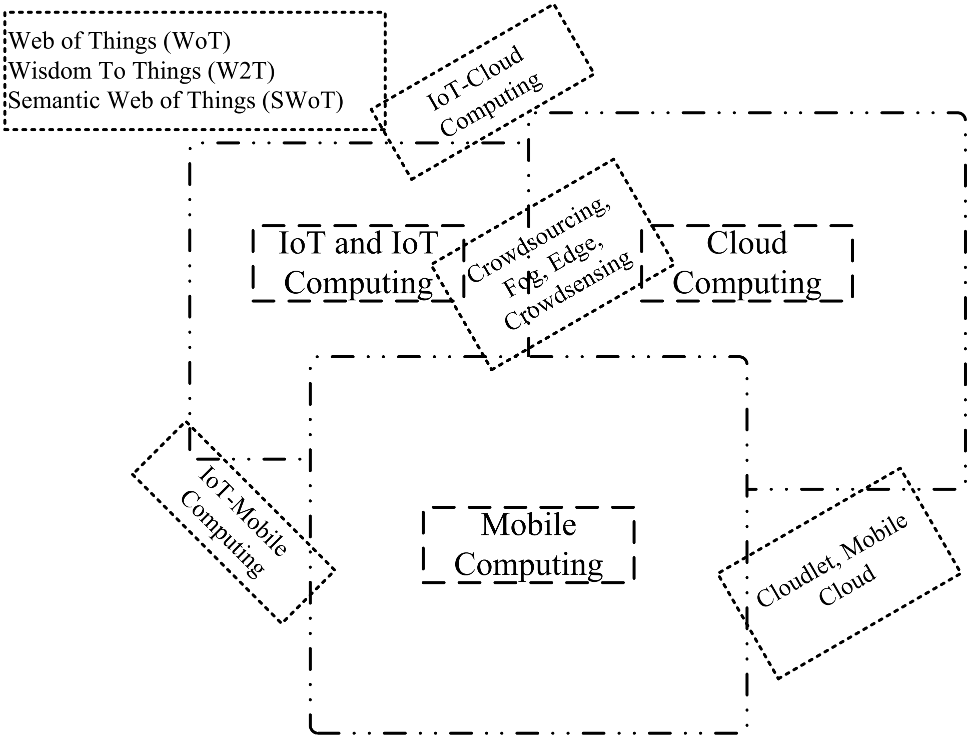


Fig. 2 Intersection areas of emerging computing paradigms

Table 1 Key challenges of the related existing works

Existing schemes	Technique used	Sensor compatibility	Major contribution	Research gaps
Alam et al. [27]	IoT, personalized healthcare	No	It emerges the application standards and communication technologies	It does not have any specific strategy to solve the security issues
Balli et al. [28]	IoT, electronic healthcare design	Partial	It has a processing system to analyze the sensory features	It does not have any futuristic concepts to design an effective system
Chandhuri et al. [29]	IoT, healthcare management	No	It has a strong analysis to examine data management systems	It does not have any security aspects to infer the difficulties of medical sensors
Suguna et al. [30]	IoT, healthcare diagnostics	No	It provides a substantial idea to analyze the cloud-based Io	It does not have any specific sensors to analyze the features of smart securities
Gandhi et al. [31]	IoT, intelligent healthcare	No	It has an intelligent healthcare system to study the integrity issues of IoT	It does not have any specific analysis to analyze the weakness of healthcare systems
Khan et al. [32]	IoT, elderly healthcare	No	It discusses the practical issues of IoT healthcare systems	It does not have any specific integration to examine the performance efficiency
Darshan et al. [33]	Healthcare IoT	No	It has a framework, design strategy, and challenges to discuss the application scenario of IoT	It does not have any valuable aspects to leverage the challenges of smart healthcare
Deebak et al. [34]	IoT, cloud, healthcare	Yes	It has a smart authentication framework to verify security features	It has some challenges to address such as privacy preservation
Deebak et al. [35]	Smart IoT, mobile-sink	Yes	It has a lightweight authentication model to examine features of IoT assisted systems	It has some security challenges such as user anonymity and privileged-insider
Deebak et al. [36]	IoT, cloud, edge computing	Yes	It has a seamless authentication framework to meet the objectives of mobile edge computing	It has some performance efficiencies including computation and storage
Al-Turjman et al. [6]	IoT, big-data, industrial systems	Yes	It has a seamless framework to examine the challenges of smart industrial applications	It does not have any specific strategy to meet the objectives of big-data technologies

features. Darshan et al. [33] examined the novel frameworks and challenges to investigate the challenges. Deebak et al. [34] designed a smart mutual authentication protocol for cloud-based medical healthcare. Deebak et al. [35] introduced a lightweight authentication framework for smart IoT system. Deebak et al. [36] presented a seamless authentication mechanism for edge computing systems. Al-Turjman et al. [6] proposed an intelligent authentication for smart industrial system.

Related works

A theory, known as Chebyshev chaotic map is widely employed for cryptography systems i.e. for S-boxes and hashing function. Lately, the client–server authentication protocols have been adopted using TMIS [37]. In 2010, Guo and Zhang [38] proven that Xiao et al. [39] is still susceptible to server-spoofing attack. In 2012, Xue et al. [40] presented an extended version of the authentication protocol using a chaotic map. Tan [41] demonstrated that Xue et al. scheme is vulnerable to man-in-the-middle attack with inadequate user anonymity. In 2013, Guo et al. [42] introduced a chaotic-map based authentication scheme using a smartcard. However, Hao et al. [43] found that Guo et al. cannot offer user untraceability. In addition, they consume two secret-key to provide more computation overhead. To address effectively, an extended version was proposed. Jiang et al. [44] and Lee [45] shown the security weaknesses of Hao et al. namely stolen smartcard attack. Subsequently, they presented the extended version of the authentication mechanism for TMIS. Mishra et al. [46] demonstrated the security deficiency of Jiang et al. such as the desynchronization attack, which may lack the order of continuity. This attack may infer the user information that demonstrates the occurrence of the next successive session of the participants to experience the DoS attack i.e. to block the execution of user authentication.

Li et al. [47] discovered that schemes such as Jiang et al. [44] and Lee [45] were found to be insecure in the user authentication process. In 2014, Lin proposed a dynamic-identity based authentication protocol using a chaotic-map. Unfortunately, Wang et al. [48] demonstrated that the Li et al. scheme is still insecure to provide user anonymity and key impersonation attack. Subsequently, they presented an extended version using mobile-device and chaotic-map for the TMIS. However, Bergamo et al. [49] are vulnerable to offline guessing, key impersonation, and desynchronization attack. Moreover, the Wang et al. scheme cannot provide session-key agreement and user anonymity. In 2015, Lee [50] cannot be resisting the offline key guessing attack. In 2016, Islam et al. [51] demonstrated the security weakness of user anonymity, key impersonation, and forward secrecy existing in Lin scheme [52]. Also, Liu and Xue [53] projected that the Lee scheme [50] was complex to design asymmetric encryption. However, the Liu and Xue scheme has a security weakness containing no password friendliness and user anonymity.

To administrate the service providers and service access, medical applications should maintain a reliable database system. It applies two-factor or three-factor authentication mechanisms to offer a systematic registration procedure that allows smart devices to acquire system access from the available network providers. As a result, data redundancy or duplication may be prevented to improve system performance. Deebak et al. [7] designed a dynamic identity-based authentication for TMIS, which preserves the medical data and avoids the clock un-synchronization to prevent potential threats. Of late, several dynamic authentication mechanisms [7, 52] have been considered for the improvisation of security efficiencies and minimization of system computation cost. However, their schemes cannot support multi-server architecture to improve system performance.

Madhusudhan et al. [54] and Biswas et al. [55] have presented static and dynamic identity-based authentication for the enrichment of security efficiencies. The former strategy prevents data leakage, whereas the latter applies a two-factor strategy including device identity and secret key to provide to serve remote-server authentication. As a consequence, several dynamic-identity based authentication mechanisms have been presented for the preclusion of client anonymity [56]. These schemes frequently change client identities using the login and authentication phase to prevent data disclosure and stolen-verifier. However, the remote-server cannot employ password-based authentication to preserve user identities and passwords during the login phase. Since the application and its related services may grow exponentially in real-time, a suitable dynamic identity-based authentication is considered to improve the efficiency factors of the server. It has a service provider that uses a multi-server environment to provide seamless connectivity [26]. In the client registration, each phase executes the authentication module to improve the security efficiencies.

As the application device repetitively invokes the login phase, it can easily be prone to data duplication and information leakage. Most importantly, cloud servers offer IoT services to real-time users over an insecure wireless channel that highly demands data confidentiality to authenticate the service access in IoT-based cloud computing systems. It uses trusted third parties to authorize the user access that obtains the IoT services through the knowledge of the cloud server. It has a registration center to restrict the service access between the cloud server and smart device. It may achieve a proper mutual authentication to secure the communication channel to acquire: (1) the device or user terminal should be legal to gain the server access; (2) the service provider should authenticate the application services to improve system efficiencies; and (3) the client device has a common session key to preserve data confidentiality and user privacy [57].

In eHealth, the IoT-based cloud computing systems should have essential characteristics of the security framework to analyze the vulnerabilities and threats [58]. It has a robust security mechanism to protect network access. The system layer handles the privacy issues proactively to enhance the feature of privacy protection. The eHealth has medical experts and service providers to store the sensitive information of the patients on the local system [59]. It demands an effective infrastructure to exchange the medical data between a patient and medical experts while patient privacy is guarded. The system deployment measures privacy awareness to classify the nature of potential risks, which comply with industrial standards, framework, regulation, and ethical requirements. To provide an effective design, the IoT applications integrate the privacy framework. It can apply the technical strategies including identification, authentication, and authorization to improve the property of data privacy. Most of the healthcare applications integrate IoT and cloud computing to signify the purpose of state definition, cluster formation, device category, and dimensional access [60]. The general security and privacy concerns are as follows:

1. In accordance with the rules and regulations, the patient data should be gathered and processed promptly to ensure device safety and liveliness.
2. Without proper privacy protection and adequate security strength, the patient data cannot be accessible over any public or private network.
3. The IoT device should process data transmission over any network access without compromising the data integrity and reliability.
4. The communication network and application devices should provide comprehensive protection to prevent unauthorized access.

5. The authorized applications should employ defined data protocols to restrict data collection and transmission.

Important key notations

The important key parameters of the proposed single user sign-in (S-USI) are illustrated in Table 2. The tabulation is as follows:

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:

$$T_n(x) = \cos n\theta, \text{ where } x = \cos\theta$$

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:

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

This assumption also defines the chaotic property of Chebyshev polynomial, where $n > 1$ represents a polynomial map $T_n : [-1, 1] \to [-1, 1]$ for the degree $\langle n \rangle$ with its relevant invariant density: $f^*(x) = {}^1\big/_{(\pi \cdot \sqrt{(1-x^2)})}$, for an exponent of Lyapunov i.e. $\ln n > 0$ [61].

Zhang [63] improved the authentication protocol using Chebyshev chaotic-map to prevent the security weakness demonstrated by Bergamo et al. [49]. To strengthen the security mechanism, the Bergamo et al. extended the Chebyshev polynomial to satisfy the properties of semi-group and commutative i.e. in the interval of $\langle -\infty, \infty \rangle$ [62]. The expression is as follows:

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

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

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

This improved Chebyshev chaotic-map shows the assumptions of discrete logarithm and Diffie Hellman [63]. The basic mathematical assumptions are as follows:

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 $A_{\mathrm{dv}}^{\mathrm{DLP}}$ may try to solve the extended Chebyshev chaotic-map-based DLP i.e. computationally negligible.

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 $A_{\mathrm{dv}}^{\mathrm{CDHP}}$. Therefore, 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 hold or impracticable. The benefit is that A_{dv} can solve the problem of extended Chebyshev chaotic-map based decisional Diffie-Hellman problem, denoted as $A_{\mathrm{dv}}^{\mathrm{DDHP}}$. Therefore, it is computationally negligible.

Table 2 System parameters used in proposed S-USI

Parameters	Description
U_{sr}	User
U_{id}	Identity of U_{sr}
P_{wd}	Password of U_{sr}
R_{S}	A remote server holds the registration of U_{sr}
TS_1	User timestamp
TS_2	Server timestamp
Δ_{TS}	Timestamp threshold
$E_{\mathrm{k}}(.)/D_{\mathrm{k}}(.)$	Apply encryption and decryption algorithm to secure the session with secret-key s_{k}
λ	Generation of Session key between U_{sr} and R_{S}
l_{g}	Size of the secure parameter
$h(.)$	One-way hash function, which is $h: \{0,1\}^* \to \{0,1\}^{l_{\mathrm{g}}}$
$H(.)$	One-way hash function, which is $H : \{1,-1\}^* \to \{0,1\}^{l_{\mathrm{g}}}$
$X \to Y : M_{\mathrm{sg}}$	X sends the transmission message M_{sg} to Y over a common wireless channel
$M_{\mathrm{sg1}} \parallel M_{\mathrm{sg2}}$	Transmission message M_{sg1} concatenates the another message M_{sg2}

Attacker model

As referred to [64], an adversary A_{dv} is supposed to have the following essential abilities informally. This is to note that this paper does not primly focus on how A_{dv} can achieve the security goals, but the examination is only assumed to results analysis, which can be:

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 to retrieve the confidential information from the stolen device [65].
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 [66].
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 [67].
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 $1/2^{6n}$ [68] i.e. for n character long-string.
7. To achieve the property of forward secrecy demonstrated in [69], 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.

Proposed single user sign-in (S-USI) mechanism

This section presents a proposed S-USI mechanism that is completely based on the extended Chebyshev chaotic-map. As the 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 cannot compute a shared session-key to establish secure communication between the user and the remote server to forge a valid request message or impersonate as a legal user. Moreover, in the secret-key update phase of S-USI, the timestamp always guarantees the data freshness to validate the data from the remote server. Thus, the proposed S-USI can prevent privileged-insider, redirection, and a data forgery attack. This proposed scheme comprises of five communication phases, such as system initialization, registration, login and authentication, secret key update, and smartcard revocation. 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 to maintain a smartcard revocation during the system initialization phase.

Assume G, g and q are defined to the parameters of the cyclic group. It has a public key encryption PE_k, secure-session key SS_k, $\mathrm{PE}_k^{'}$(Conjugate of PE_k), $\mathrm{SS}_k^{'}$ (Conjugate of SS_k) and multimedia server M_{S}. Moreover, it maintains a long-term secret key S_k with a random string length k. Let $H : \{0,1\}^* \rightarrow \{0,1\}^k$ represents a one-way hash function to prevent target collision, whereas $\mathrm{PRF}_{S_k} : \{0,1\}^k \rightarrow \{0,1\}^k$ denotes a pseudo-random function key. Also a one-way hash (conjugate) function $H' : \{0,1\}^* \rightarrow \{0,1\}^k$ is defined to preserve client identities. In S-USI, $H'(S_k)$ assumes S_k as an input key to initiate the authentication procedure.

System initialization phase Remote-server R_{S} builds a system communication parameters to perform the following execution steps:

Step 1 R_{S} chooses a random integer p_k to define a private secret-key that has a random computation parameter $x \in \langle -1, +1 \rangle$.

Step 2 R_{S} generates a master secret-key m_{sk} that applies a secure symmetric encryption and decryption algorithm, which is $E_k(.)/D_k(.)$ and one-way hash operation function $h(.)$.

System registration phase R_{S} issues a secure communication gateway to the multimedia device M_{d}/medical sensor M_{s} to guarantee key security and data privacy.

Step 1 M_{d}/M_s arbitrarily chooses an identity of unary-token I_{d} along with user identity U_{id} and secret password P_{wd} and then sends the identity I_{d} to R_{S} over public access networks.

Step 2 In pursuit of receiving I_{d}, M_{S} determines $\mathrm{key} = \mathrm{PRF}_{S_k}(H(I_{\mathrm{d}})) \oplus H'(S_{k_0})$, $R = E_{\mathrm{S}}(I_{\mathrm{d}} \parallel H)$ and $D = H \oplus (x \parallel T_r(x))$ using m_{sk} where S_{k_0} is a session key to validate whether it is newly generated or not to authorize user access.

Step 3 R_{S} connects an authentic gateway, which has the system parameters as $I_{\mathrm{d}}, \mathrm{Key}, R, D, h(.), E_k(.)$ to setup a connection. In practice, the system parameters are predefined to exclude any additional key exchanges to secure gateway access. As a result, the gateway is equipped to configure with any M_d/M_s to store the communication parameters in the smartcard S_C.

Step 4 Upon the successful configuration, the client devices namely M_d/M_s setup a session-key to confirm the user privacy to R_S over a secure gateway.

System login and key-authentication phase user namely M_d/M_s enters a secret session-key to access the private information of patients. A secure gateway retrieves the value of the secret session-key $\text{Key}_{\text{verif}} = \text{Key}_1 \oplus H'(S_k)$. Then, the users' and M_s use $\text{Key}_{\text{verif}}$ as the secret-key to perform the following computation (Fig. 3):

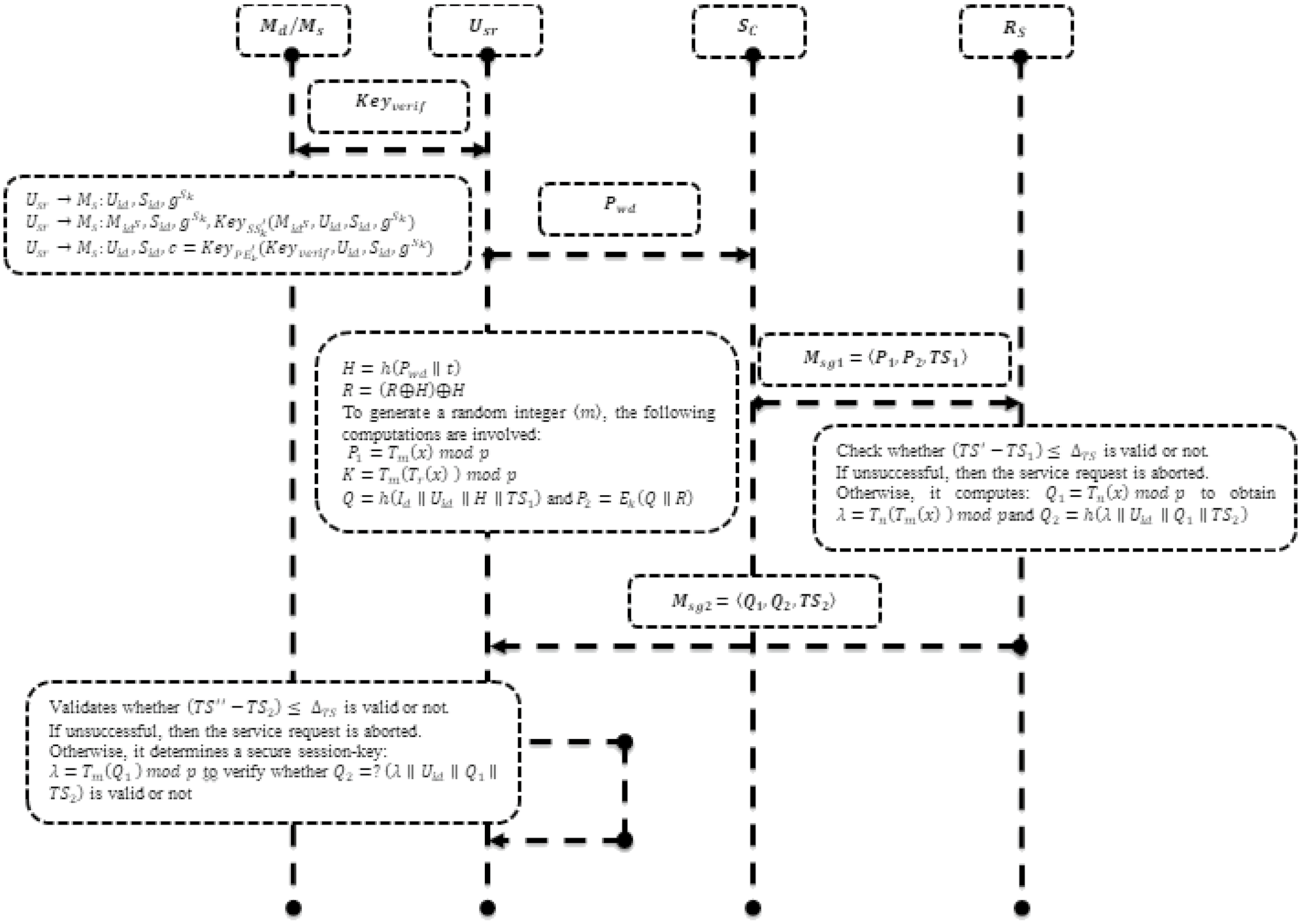
$$U_{sr} \to M_s : U_{id}, S_{id}, g^{S_k}$$

$$U_{sr} \to M_s : M_{id}{}^{s}, S_{id}, g^{S_k}, \text{Key}_{SS'_k}(M_{id}{}^{s}, U_{id}, S_{id}, g^{S_k})$$

$$U_{sr} \to M_s : U_{id}, S_{id}, c = \text{Key}_{PE'_k}(\text{Key}_{\text{verif}}, U_{id}, S_{id}, g^{S_k})$$

Step 1 U_{sr} inserts his/her S_C to provide an input P_{wd} to compute $H = h(P_{wd} \parallel t)$ and $R = (R \oplus H) \oplus H$. The above computation is used to generate a random integer m that computes $P_1 = T_m(x) \mod p$, $K = T_m(T_r(x)) \mod p$, $Q = h(I_d \parallel U_{id} \parallel H \parallel \text{TS}_1)$ and $P_2 = E_k(Q \parallel R)$, where TS_1 is the current timestamp. Finally, the communication parameters $M_{sg1} = \langle P_1, P_2, \text{TS}_1 \rangle$ are dispatched to R_S.

Step 2 Upon receiving the message transmission M_{sg1}, R_S checks whether $(\text{TS}' - \text{TS}_1) \leq \Delta_{\text{TS}}$ is valid or not. If the message transmission is unsuccessful, then R_S aborts the service request. Otherwise, R_S determines $K = T_r(P_1) \mod p$ to obtain $(Q \parallel R)$ by the decryption process P_2 with K. In addition, it obtains $(U_{id} \parallel H \parallel C_{NT})$ by the process of decryption with m_{sk}. Then, R_S verifies whether (U_{id}, C_{NT}) is stored in the revocation table or not to examine $Q = ?h(I_d \parallel U_{id} \parallel H \parallel \text{TS}_1)$. If the verification is unsuccessful, then R_S simply rejects the service authentication request. Otherwise, R_S generates a random integer n to compute $Q_1 = T_n(x) \mod p$ to obtain $\lambda = T_n(T_m(x)) \mod p$ and $Q_2 = h(\lambda \parallel U_{id} \parallel Q_1 \parallel \text{TS}_2)$, where TS_2 is the current server



M_d/M_s
U_{sr}
S_C
R_S
Key_{verif}
$U_{sr} \to M_s: U_{id}, S_{id}, g^{S_k}$
$U_{sr} \to M_s: M_{id}{}^{s}, S_{id}, g^{S_k}, Key_{SS'_k}(M_{id}{}^{s}, U_{id}, S_{id}, g^{S_k})$
$U_{sr} \to M_s: U_{id}, S_{id}, c = Key_{PE'_k}(Key_{verif}, U_{id}, S_{id}, g^{S_k})$
P_{wd}
$H = h(P_{wd} \parallel t)$
$R = (R \oplus H) \oplus H$
To generate a random integer (m), the following computations are involved:
$P_1 = T_m(x) \mod p$
$K = T_m(T_r(x)) \mod p$
$Q = h(I_d \parallel U_{id} \parallel H \parallel TS_1)$ and $P_2 = E_k(Q \parallel R)$
$M_{sg1} = (P_1, P_2, TS_1)$
Check whether $(TS' - TS_1) \leq \Delta_{TS}$ is valid or not.
If unsuccessful, then the service request is aborted.
Otherwise, it computes: $Q_1 = T_n(x) \mod p$ to obtain $\lambda = T_n(T_m(x)) \mod p$ and $Q_2 = h(\lambda \parallel U_{id} \parallel Q_1 \parallel TS_2)$
$M_{sg2} = (Q_1, Q_2, TS_2)$
Validates whether $(TS'' - TS_2) \leq \Delta_{TS}$ is valid or not
If unsuccessful, then the service request is aborted.
Otherwise, it determines a secure session-key:
$\lambda = T_m(Q_1) \mod p$ to verify whether $Q_2 = ?(\lambda \parallel U_{id} \parallel Q_1 \parallel TS_2)$ is valid or not

Fig. 3 Flow mechanism of proposed S-USI during system login and authentication

timestamp. Finally, R_S dispatches $M_{sg2} = \langle Q_1, Q_2, TS_2 \rangle$ to U_{sr}.

Step 3 After receiving the message transmission M_{sg2}, U_{sr} validates whether $(TS'' - TS_2) \le \Delta_{TS}$ is valid or not. If the validation was unsuccessful, then U_{sr} terminates the user authentication request. Otherwise, U_{sr} determines a secure session-key $\lambda = T_m(Q_1) \mod p$ to verify whether $Q_2 = ?(\lambda \parallel U_{id} \parallel Q_1 \parallel TS_2)$ is valid or not. If unsuccessful, U_{sr} terminates the user authentication request.

System secret-key update phase In this secret-key update phase, a legitimate user U_{sr} inserts his/her S_C to enter the old secret-password P_{wd} to change or modify into new secret-password P^*_{wd}. The execution steps are as follows:

Step 1 S_C performs a computation of $H = h(P_{wd} \parallel t)$ and $H^* = h(P^*_{wd} \parallel t)$ to generate a random integer m to recalculate $P_1 = T_m(x) \mod p$, $K = T_m(T_r(x)) \mod p$, $Q = h(I_d \parallel U_{id} \parallel H \parallel TS_1)$, $R = (R \oplus H) \oplus H$ and $P_2 = E_k(H^* \parallel Q \parallel R)$, where TS_1 is the current timestamp. Lastly, $M_{sg1} = \langle P_1, P_2, TS_1 \rangle$ are dispatched to R_S to choose a new secret key S'_k.

Step 2 Upon receiving the message transmission M_{sg1}, R_S verifies whether $(TS' - TS_1) \le \Delta_{TS}$ is valid or not. If the message transmission is unsuccessful, then R_S aborts the service request. Otherwise, R_S determines $K = T_r(P_1) \mod p$ to obtain $(Q \parallel R)$ by the decryption process P_2 with K. In addition, it obtains $(U_{id} \parallel H \parallel C_{NT})$ by the process of decryption with m_{sk}. Then, R_S verifies whether (U_{id}, C_{NT}) is stored in the revocation table or not to examine $Q = ?h(I_d \parallel U_{id} \parallel H \parallel TS_1)$. If the verification is unsuccessful, then R_S simply rejects the service authentication request. If the authentication is successful, then R_S determines $R^* = E_S(I_d \parallel U_{id} \parallel H^* \parallel C_{NT})$, $Q_1 = (Q \oplus R^*)$ and $Q_2 = h(K \parallel H^* \parallel R^* \parallel TS_1)$. Finally, $M_{sg2} = \{Q_1, Q_2\}$ is transmitted to S_C.

Step 3 After receiving M_{sg2}, S_C computes $R^* = (Q \oplus Q_1)$ to verify whether $Q_2 = ?h(K \parallel H^* \parallel R^* \parallel TS_1)$ is valid to compute $\text{Update}_{key} = \text{Key}_1 \oplus H'(S_k) \oplus H'(S'_k)$, where S_k is the old secret key. If the validation is successful, then S_C replaces Key_1 with Update_{key} and $(R \oplus H)$ with $(R^* \oplus H^*)$.

Smartcard revocation phase In this phase, a legitimate user wishes to revoke his/her S_C to obtain a new S_C. The execution steps are as follows:

Step1: U_{sr} enters his/her user identity U_{id} and secret password P_{wd} to choose a random integer t_{New} to compute $H_{New} = h(P_{wd} \parallel t_{New})$ that is finally dispatched the communication parameters $\langle U_{id}, H_{New}, SC_{Revocation} \rangle$ to R_S over a public access network.

Step 2 R_S tries to determine $\langle U_{id}, C_{NT} \rangle$ from the revocation table to compute $C^{New}_{NT} = C_{NT} + 1$ and $R^{new} = E_S(U_{id} \parallel H_{New} \parallel C^{New}_{NT})$ using a master secret-key m_{sk}. Finally, the computation parameters $\left\langle U_{id}, C^{New}_{NT} \right\rangle$ is stored in its revocation table.

Step 3 R_S records $\langle R^{new}, h(.), E_k(.), x, T_r(x) \rangle$ into S_C that issues S_C to U_{sr} over a public access network.

Step 4 Upon receiving S_C, U_{sr} inserts t_{New} to perform the smartcard revocation phase.

Security analysis

This section demonstrates the security analysis of the proposed S-USI mechanism using AKE session-key security and BAN logic. That not only complies with key properties such as mutual authentication and session key agreement but also resilient to the potential attacks such as redirection, replay, forgery, and privileged-insider.

Providing AKE session-key security

The proposed S-USI mechanism reveals that it could provide better session-key security to adopt the models namely real-or-random (RoR) and sequence of the game (SoG) [70, 71]. A Difference Lemma [72] is employed for the game sequence that is as follows:

Lemma 1 (Difference Lemma) *Assume that X, Y and F be the sequence of events that defines the distribution probability. It is supposed that $X \wedge \neg F \Leftrightarrow B \wedge \neg F$. It can be expressed as:*

$$|Pr[X] - Pr[Y]| \le Pr[F]$$

Therefore, the above theorem shows that the proposed S-USI mechanism has the AKE session-key security if the extended Chebyshev chaotic-map based DDHP adheres.

Theorem 1 *The distribution probability D_P demonstrates that A_{dv} may wish to terminate the AKE session key security of proposed S-USI to satisfy:*

$AD^{AKE}_P \le 2 \cdot AD^{DDHP} + \frac{2}{N} + \frac{1}{2^{(l-1)}}$, *where* AD^{DDHP} *represents the advantage factor that the extended Chebyshev chaotic-map based* DDHP *wishes to solve the defined size of P_{wd} list and secure parameter l.*

Proof GM^{AKE}_i is a game probability to define the concurrent events E_i that represents the adversary to win the game. GM^{AKE}_0 signifies the starting of the game to denote a real-time attack opposed to the proposed S-USI mechanism and GM^{AKE}_1 indicates the end of the game to gain or break the AKE Session-Key Security of the proposed S-USI mechanism.

GameGM$^{AKE}_0$ This game represents the real-time attack that is defined as:

$$\mathrm{AD}_{\mathrm{P}}^{\mathrm{AKE}}(A) = \left|2 \cdot \Pr\left[E_0\right] - 1\right| \tag{1}$$

GameGM$_1^{AKE}$ This game corresponds to the parallel-guessing attack. Assume that each $P_2 = E_k(Q \parallel R)$ is completely dissimilar where $Q = h(I_{\mathrm{d}} \parallel U_{\mathrm{id}} \parallel H \parallel \mathrm{TS}_1)$, $H = h(P_{\mathrm{wd}} \parallel t)$ and $K = T_m(T_r(x)) \mod p$ to select the random integers t and m provided by U_{sr} and the current timestamp TS_1. Therefore, A_{dv} has no U_{sr} information to guess the P_{wd}. This analysis proves that the resilient to the password-guessing attack is evaluated by the given probability that defines the message transmission $P_2 = E_k(Q \parallel R)$ to indicate whether the password-guessing is correct. Thus, it is said to be:

$$\left|\Pr\left[E_0\right] - \Pr\left[E_1\right]\right| \le \frac{1}{N} \tag{2}$$

GameGM$_2^{AKE}$ This game considers the transformation of $\mathrm{GM}_1^{\mathrm{AKE}}$ into $\mathrm{GM}_2^{\mathrm{AKE}}$ to choose a random integer in place of computing a hash function. Subsequently, $\mathrm{GM}_1^{\mathrm{AKE}}$ and $\mathrm{GM}_2^{\mathrm{AKE}}$ are excepted to be indistinguishable excluding the collision hash function $\mathrm{GM}_2^{\mathrm{AKE}}$. According to birthday-paradox [70] and Lemma 1, it has:

$$\left|Pr\left[E_1\right] - Pr\left[E_2\right]\right| \le \frac{1}{2^l} \tag{3}$$

GameGM$_3^{AKE}$ This game considers $\mathrm{GM}_2^{\mathrm{AKE}}$ to transform using triple samples X, Y, Z that defines a random distribution $T_m(x) \mod p, T_n(x) \mod p, T_z(x) \mod p$ rather than the extended Chebyshev chaotic-map based DDHP. $\mathrm{GM}_2^{\mathrm{AKE}}$ is thus similar to $\mathrm{GM}_3^{\mathrm{AKE}}$ to define:

$$\Pr\left[E_2\right] = \Pr\left[E_3\right] \tag{4}$$

Assume that a challenger $\mathrm{CH}_{\mathrm{DDHP}}$ tries to disrupt the indistinguishability of extended Chebyshev chaotic-map based DDHP and $A_{\mathrm{dv}}^{\mathrm{AKE}}$ be denoted to break up the property of session-key security. $\mathrm{CH}_{\mathrm{DDHP}}$ yields the real-key λ to $A_{\mathrm{dv}}^{\mathrm{AKE}}$ if the unbiased coin returns a bit $\langle c = 1\rangle$. Otherwise, $\langle c = 0\rangle$ is returned to execute a random-string i.e. for $A_{\mathrm{dv}}^{\mathrm{AKE}}$. Subsequently, $A_{\mathrm{dv}}^{\mathrm{AKE}}$ returns the output function to guess a bit $\langle c'\rangle$ to win a game if $\langle c' == c\rangle$. $A_{\mathrm{dv}}^{\mathrm{DDHP}}$ executes the output exactly as defined in the proceeding experiment excluding $\langle X, Y, Z\rangle$, which is defined to be an input variable. If $A_{\mathrm{dv}}^{\mathrm{AKE}}$ executes the output function $\langle c\rangle$, then $A_{\mathrm{dv}}^{\mathrm{AKE}}$ returns the output $\langle 1\rangle$. Otherwise, it returns the output $\langle 0\rangle$. If $\langle X, Y, Z\rangle$ is considered to be a real extended Chebyshev chaotic-map based DDHP, then $\mathrm{A}_{\mathrm{dv}}^{\mathrm{DDHP}}$ executes $A_{\mathrm{dv}}^{\mathrm{AKE}}$ in $\mathrm{GM}_3^{\mathrm{AKE}}$. Thus, it equals $\Pr\left[\text{Event that } A_{\mathrm{dv}}^{\mathrm{DDHP}} \text{executes} \langle 1\rangle\right]$ with $\Pr\left[E_3\right]$. If $\langle X, Y, Z\rangle$ is defined to be a random triple variable, then $A_{\mathrm{dv}}^{\mathrm{DDHP}}$ executes an output function $A_{\mathrm{dv}}^{\mathrm{AKE}}$ to equate $\Pr\left[\text{Event that } A_{\mathrm{dv}}^{\mathrm{DDHP}} \text{executes } \langle 1\rangle\right]$ with $\Pr\left[E_4\right]$. Thus, it is defined as:

$$\left|\Pr\left[E_3\right] - \Pr\left[E_4\right]\right| \le \mathrm{AD}^{\mathrm{DDHP}}(A_{\mathrm{dv}}^{\mathrm{DDHP}}) \tag{5}$$

Eventually, it claims that no information message about unbiased coin bit $\langle c\rangle$ is disclosed to infer the secret session-key including random and independent variables of the proposed S-USI scheme. It is defined as:

$$\Pr\left[E_4\right] = \frac{1}{2} \tag{6}$$

Using Lemma 1, the above Eqs. (1) to (6) can be combined to yield:

$$\mathrm{AD}_{\mathrm{P}}^{\mathrm{AKE}}(\mathrm{A}_{\mathrm{dv}}^{\mathrm{AKE}}) \le 2 \cdot \mathrm{AD}^{\mathrm{DDHP}} + \frac{2}{N} + \frac{1}{2^{(l-1)}}$$

Hence, the proof is resolved.

Providing a property of session-key agreement The proposed S-USI scheme adheres with the property of proper session-key agreement.

Proof By the above Theorem 1, the security of session-key agreement is completely based on extended Chebyshev chaotic-map based DDHP to avoid the security weaknesses provided in Bergamo et al. [49]. Thus, it can be neither U_{sr} nor R_{S} to determine a session-key S_k to satisfy the property of the session-key agreement.

Resilient to replay attack The proposed S-USI scheme provides a secret-key update phase to resist the replay attack.

Proof In the S-USI scheme, a secret-key update phase uses S_{C} to transmit the message transmission $M_{\mathrm{sg1}} = \langle P_1, P_2, \mathrm{TS}_1\rangle$ i.e. to R_{S}, where TS_1 is the current timestamp, $P_1 = T_m(x) \mod p$, $K = T_m(T_r(x)) \mod p$ and $Q = h(I_{\mathrm{d}} \parallel U_{\mathrm{id}} \parallel H \parallel \mathrm{TS}_1)$. From the verification of timestamp TS_1 and $Q = ?h(I_{\mathrm{d}} \parallel U_{\mathrm{id}} \parallel H \parallel \mathrm{TS}_1)$, the key freshness of message transmission can be obtained. Thus, the proposed S-USI mechanism can restrict the replay attack.

Resilient to denial-of-service attack The proposed S-USI scheme provides a secret-key update phase to resist the denial-of-service (DoS) attack.

Proof Since S_{C} verifies the updated data R^* by validating on $Q_2 = h(K \parallel H^* \parallel R^* \parallel \mathrm{TS}_1)$ to substitute R with R^* where TS_1 is the current timestamp generated by S_{C} to produce $H^* = h(P_{\mathrm{wd}}^* \parallel t)$. It is claimed that none of the A_{dv} can modify the response message $M_{\mathrm{sg1}} = \langle P_1, P_2, \mathrm{TS}_1\rangle$. Hence, the proposed S-USI mechanism can prevent the denial-of-service attack.

Resilient to privileged-insider attack The proposed S-USI scheme provides a secret-key update phase to resist the privileged-insider attack.

Proof In S-USI, each legitimate user has $(x, T_r(x))$ in S_C that is based on extended Chebyshev chaotic-map based DDHP that strengthen the session-key agreement. Therefore, A_dv could not derive a secret key s_k and a session-key S_k which is mutually communicated between another U_sr and R_S during authenticated and key agreement and secret-key update phase. The analysis proves that none of the A_dv can receive $(Q \parallel R)$ and $(U_\mathrm{id} \parallel H \parallel C_\mathrm{NT})$ during the authentication and key agreement phase; $(H^* \parallel Q \parallel R)$ and $(U_\mathrm{id} \parallel H \parallel C_\mathrm{NT})$ during the secret-key update phase. It is claimed that U_sr has much difficult to forge a valid request message to impersonate as a legitimate user. Therefore, the proposed S-USI mechanism is resilient to privileged-insider attack.

Client anonymity and identity protection For any devices $M_\mathrm{d}/M_\mathrm{s}$, the proposed S-USI substitutes I_d instead of client identities $U_\mathrm{id}/S_\mathrm{id}$. As it applies a pseudonym identity for the client devices, A_dv may not compute a real identity of any communication devices until the unary identity verification is successfully passed.

Moreover, the pseudonym identities generate a valid session key for both server and clients $M_\mathrm{d}/M_\mathrm{s}$, neither the client nor server may compute the real identities to establish a secure session of each other. This strategy is applied to restrict the information leakage between the client devices and server to A_dv. Thus, the proposed S-USI can adhere to the properties of client anonymity and identity protection.

Traceability The existing authentication protocols [16, 19, 20] cannot offer a reliable feature of traceability as the pseudo-identities are known to the communication network. However, the proposed S-USI can compute the real identities of client/server to protect the pseudonym identities when $M_\mathrm{d}/M_\mathrm{s}$ derives the anonymity function using key $= \mathrm{PRF}_{S_k}(H(I_\mathrm{d})) \oplus H'(S_{k_0})$. Hence, the proposed S-USI mechanism offers the feature of traceability to verify the genuineness of application service.

Mutual authenticity Using system authentication, the proposed S-USI claims that it can offer a property mutual authentication between the client devices $M_\mathrm{d}/M_\mathrm{s}$. To confirm the legitimacy, $\mathrm{Key}_\mathrm{verif} = \mathrm{Key}_1 \oplus H'(S_k)$ is utilized. Besides, the key derivatives namely $\mathrm{Key}_{\mathrm{SS}'_k}(M_{\mathrm{id}^\mathrm{s}}, U_\mathrm{id}, S_\mathrm{id}, g^{S_k})$ and $\mathrm{Key}_{\mathrm{PE}'_k}(\mathrm{Key}_\mathrm{verif}, U_\mathrm{id}, S_\mathrm{id}, g^{S_k})$ are executed to achieve a process of key validation. Thus, the proposed S-USI offers a feature of mutual authentication to gain legitimacy access.

Secret session key agreement To offer data protection between the devices and servers, the proposed S-USI determines $Q_2 = h(\lambda \parallel U_\mathrm{id} \parallel Q_1 \parallel \mathrm{TS}_2)$ over a public network. It uses a valid secret key to be shared between the devices remotely. As a result, the proposed S-USI embeds a tightly coupled hashing key $= \mathrm{PRF}_{S_k}(H(I_\mathrm{d})) \oplus H'(S_{k_0})$ to protect the end-to-end connectivity. Hence, the proposed S-USI achieves secret session key agreement with firmness between the devices $M_\mathrm{d}/M_\mathrm{s}$.

Secret key update/change In the phase of secret-key update/change, the users may change his/her secret key by the execution of $\mathrm{Update}_\mathrm{key} = \mathrm{Key}_1 \oplus H'(S_k) \oplus H'(S'_k)$. It will later affect the parameters, such as $\mathrm{PE}_k, \mathrm{PE}'_k, I_\mathrm{d}, \mathrm{Key}, p, g, q$ to verify and validate the data transmission of the users. Thus, the proposed S-USI mechanism claims that the secret key update/change to the users is safe.

Resilient to forgery and insider attack The proposed S-USI protects the device identities, whereby A_dv cannot tamper the device identities or credentials to check the data integrity. Moreover, the proposed S-USI derives the expression key $= \mathrm{PRF}_{S_k}(H(I_\mathrm{d})) \oplus H'(S_{k_0})$ to verify the secret key of the communication devices. It is noted that I_d is incorporated to protect the device access. Thus, the proposed S-USI claims that the device identities can be embedded tightly to protect the system privileges from the threats including data forgery and insider.

Resilient to Eavesdropping attack A_dv cannot infer deduce the device confidential as it may not be able to overhear/eavesdrop the device communication over a public channel. Since I_d often changes for the devices $M_\mathrm{d}/M_\mathrm{s}$, the device secret key key $= \mathrm{PRF}_{S_k}(H(I_\mathrm{d})) \oplus H'(S_{k_0})$ changes dynamically over some time during the login request.

Thus, the proposed S-USI asserts that A_dv cannot collect any previous details to interfere/eavesdrop on the public networks. Besides, A_dv cannot obtain neither key $= \mathrm{PRF}_{S_k}(H(I_\mathrm{d})) \oplus H'(S_{k_0})$ nor $\mathrm{Update}_\mathrm{key} = \mathrm{Key}_1 \oplus H'(S_k) \oplus H'(S'_k)$ to achieve transmission efficiency and data confidentiality. Hence, the proposed S-USI can resist the eavesdropping attack.

Resilient to Masquerade attack A_dv cannot infer or derive the legal credential of the device as the device identities are strongly integrated using unary identity I_d. Moreover, the communication devices verify the network access using $\mathrm{Key}_\mathrm{verif} = \mathrm{Key}_1 \oplus H'(S_k)$ to derive the logic system executions including key computation, verification, and communication to establish the services between the devices via the proposed S-USI over a public network. Thus, the proposed S-USI can protect the network from a masquerade attack.

Resilient to offline password guessing attack Suppose A_dv infers the user identities U_id from the previous session $M^\mathrm{Old}_\mathrm{sg1}$ and $M^\mathrm{Old}_\mathrm{sg2}$. Then, he/she may try to collect or guess a user password and identity such as U^*_id and P^*_wd respectively through the computation of $H = h(P_\mathrm{wd} \parallel t)$ and $H^* = h(P^*_\mathrm{wd} \parallel t)$ to generate a random integer m to recalculate $P_1 = T_m(x) \mod p$, $K = T_m(T_r(x))\mathrm{mod\ p}$, $Q = h(I_\mathrm{d} \parallel U_\mathrm{id} \parallel H \parallel \mathrm{TS}_1)$, $R = (R \oplus H) \oplus H$ and $P_2 = E_k(H^* \parallel Q \parallel R)$, where TS_1 is the current timestamp. However, the parameters known as $\langle P_1, K, Q, R, P_2 \rangle$ cannot be guessed without the proper occurrence of timestamp TS_1.

Therefore, the proposed S-USI mechanism can be resilient to an offline password guessing attack. This is also to note that after the successful inference of P^*_{wd}, A_{dv} may try to perform a computation of $H^* = h(P^*_{\mathrm{wd}} \parallel t)$ to examine $Q = ?h(I_{\mathrm{d}} \parallel U_{\mathrm{id}} \parallel H \parallel \mathrm{TS}_1)$. If the verification is unsuccessful, then R_{S} simply rejects the service authentication request. If the authentication is successful, then R_{S} determines $R^* = E_{\mathrm{S}}(I_{\mathrm{d}} \parallel U_{\mathrm{id}} \parallel H^* \parallel C_{\mathrm{NT}})$, $Q_1 = (Q \oplus R^*)$ and $Q_2 = h(K \parallel H^* \parallel R^* \parallel \mathrm{TS}_1)$ to provide authentic service access to an adversary.

Resilient to user impersonation attack To act as a legal user, A_{dv} performs a valid computation that provides an input P_{wd} to compute $H = h(P_{\mathrm{wd}} \parallel t)$ and $R = (R \oplus H) \oplus H$. The above computation is used to generate a random integer m that computes $P_1 = T_m(x) \mod p$, $K = T_m(T_r(x)) \mathrm{mod}\, p$, $Q = h(I_{\mathrm{d}} \parallel U_{\mathrm{id}} \parallel H \parallel \mathrm{TS}_1)$ and $P_2 = E_k(Q \parallel R)$, where TS_1 is the current timestamp. However, A_{dv} cannot perform a valid computation for the given expression $\{P_1, Q, P_2\}$ to pretend as a legal user. Thus, the proposed S-USI scheme claims that it can be resilient to user impersonation attack. This is also to note that A_{dv} may infer a proper timestamp TS_i and random integer x to compute: $R^* = E_{\mathrm{S}}(I_{\mathrm{d}} \parallel U_{\mathrm{id}} \parallel H^* \parallel C_{\mathrm{NT}})$, $Q_1 = (Q \oplus R^*)$ and $Q_2 = h(K \parallel H^* \parallel R^* \parallel \mathrm{TS}_1)$. Finally, a legal message transmission for U_{sr} can be determined to generate a secure session-key $\lambda = T_m(Q_1) \mod p$ to verify whether $Q_2 = ?\,(\lambda \parallel U_{\mathrm{id}} \parallel Q_1 \parallel \mathrm{TS}_2)$ is valid or not to process the service request to a remote server R_{S}.

Resilient to server-spoofing attack To act as a remote server R_{S} and forge a valid user authentic request $M_{\mathrm{sg}2}$, A_{dv} may infer a random integer p_k as a private secret-key and a master secret-key m_{sk} to perform a computation of $\mathrm{key} = \mathrm{PRF}_{S_k}(H(I_{\mathrm{d}})) \oplus H'(S_{k_0})$, $R = E_{\mathrm{S}}(I_{\mathrm{d}} \parallel H)$ and $D = H \oplus (x \parallel T_r(x))$ using m_{sk} where S_{k_0} is a session key newly generated to validate the users' identity. Thus, the proposed S-USI scheme can be free from a server-spoofing attack.

Free password selection A critical element of system login is password or user secret-key that can only be selected or updated through the authentication property of the proposed S-USI scheme by any U_{ser}. In S-USI scheme, each U_{ser} can opt for his/her password or secret-key without any limitation. However, a long-term secret key could be employed without the use of an input element when any U_{ser} tries to access the system login as referred to [71].

Construction of session-key In the execution of the system authentication phase, the proposed S-USI scheme provides access to the communication parties such as U_{ser} and R_{S} through the establishment of a secret session key. However, there would not be any secret-session key constructed for both the parties during the system authentication phase [5]. Thus, without the incorporation of session key encryption, no secure communication can be established to guarantee secure communication sessions.

Strong forward secrecy Even if A_{dv} infers the confidential information of communication parties such as U_{ser} and R_{S}, he/she could not compute $\mathrm{key} = \mathrm{PRF}_{S_k}(H(I_{\mathrm{d}})) \oplus H'(S_{k_0})$ without the knowledge of the previous timestamp TS_1 and TS_2. According to extended Chebyshev chaotic-map based DDHP, it is very hard to calculate a valid secret session-key. Table 3 shows the comparison of proposed S-USI and other related schemes with AKA security properties.

From Table 3, it is observed that various AKA security properties are cross-examined with the proposed S-USI and existing authentication scheme. Nikooghadam et al. [52] achieve the properties of session-key agreement and secret-key update and withstand the replay attack; Chaudhry et al. [53] offer the properties of session-key agreement and secret-key update; Arshad et al. [50] provide session-key agreement, secret-key update, privileged-insider, Traceability, and User Impersonation; Lu et al. [7] make available for a replay attack, privileged-insider attack, Traceability, Secret Key Update/Change, and Offline Password Guessing; Amin and Biswas [54] allow for a replay attack, Secret Key Update/Change, Offline Password Guessing Attack and Strong Forward Secrecy; and Chandrakar et al. [55] cause to achieve replay attack, privileged-insider attack, traceability, secret key update/change, offline password guessing attack, user impersonation attack, and strong forward secrecy. However, the proposed S-USI scheme can fulfill the important security properties of the AKA protocol in comparison with other authentication schemes [7, 50, 52–55].

Analysis using BAN logic

This subsection discusses a logical analysis of the proposed S-USI scheme that uses a logical tool to examine the security efficiency of cryptography protocol. Burrows et al. [76] and Buttyan et al. [77] presents a formal method to validate the mutual authentication and session-key agreement of the proposed scheme. Assume that X and Y define the principal range to determine the essential quality of a communication channel C and message transmission i.e. A and B. Table 4 shows the important notation used in the BAN logic tool.

The proposed S-USI scheme is logically described as follows:

$$\mathrm{Step1}\ :\ R_{\mathrm{S}} \triangleleft \left\langle \begin{cases} T_{\mathrm{a}}(x) \quad \mathrm{mod}\ p \\ \qquad\rightarrow \\ \mathrm{DDHP}\ \langle \mathrm{Public} \rangle \end{cases} U_{\mathrm{ser}}, C_{R_{\mathrm{S}},U_{\mathrm{ser}}}(H(I_{\mathrm{d}} \parallel U_{\mathrm{id}} \parallel H \parallel \mathrm{TS}_1), R), \mathrm{TS}_1 \right\rangle$$

Table 3 Comparison of AKE security properties with proposed S-USI and other existing schemes

Schemes properties	Nikooghadam et al. [64]	Chaudhry et al. [65]	Arshad et al. [66]	Lu et al. [67]	Amin and Biswas [69]	Chandrakar et al. [75]	Proposed S-USI Scheme
S_1	√	√	√	X	X	X	√
S_2	√	√	√	√	√	√	√
S_3	X	X	X	X	X	X	√
S_4	X	√	√	√	X	√	√
S_5	X	X	X	X	X	X	√
S_6	X	X	√	√	X	√	√
S_7	X	X	X	X	X	X	√
S_8	X	X	X	X	X	X	√
S_9	√	X	X	√	√	√	√
S_{10}	X	X	X	X	X	X	√
S_{11}	X	X	X	X	X	X	√
S_{12}	X	X	X	X	X	X	√
S_{13}	X	X	X	X	X	X	√
S_{14}	X	X	X	√	√	√	√
S_{15}	X	X	√	X	X	√	√
S_{16}	X	X	X	X	X	X	√
S_{17}	X	X	X	X	X	X	√
S_{18}	X	X	X	X	√	√	√

S_1 Providing a property of session-key agreement, S_2 resilient to replay attack, S_3 resilient to denial-of-service attack, S_4 resilient to privileged-insider attack, S_5 user anonymity and identity protection, S_6 traceability, S_7 mutual authenticity, S_8 session secret-key agreement, S_9 secret key update/change, S_{10} resilient to forgery and insider attack, S_{11} resilient to eavesdropping attack, S_{12} resilient to masquerade attack, S_{13} resilient to offline password guessing attack, S_{14} resilient to user impersonation attack, S_{15} resilient to server-spoofing attack, S_{16} free password selection, S_{17} construction of session-key, S_{18} strong forward secrecy

Table 4 Important notation used in BAN logic

Parameter	Description
$C(X)$	$\langle X \rangle$ is a message transmission, communicated over a wireless channel $\langle C \rangle$
$r(C)$	It is defined for a set of channel reader $\langle C \rangle$
$w(C)$	It is defined for a set of channel writer $\langle C \rangle$
$P\| \equiv X$	P believes a statement of the message $\langle X \rangle$
$P\| \sim X$	P read $\langle X \rangle$ once. It means that P has sent a message including of $\langle X \rangle$. The assumption is that the message is not known if P may have received a long time ago or lately. However, it is known if P believes $\langle X \rangle$
$P\| \Rightarrow X$	P provides a transmission control over $\langle X \rangle$. It means that P have a trustworthy over $\langle X \rangle \langle X \rangle$
$\#(X) : \langle X \rangle$	$\langle X \rangle$ is a fresh message transmission i.e. it has not been transmitted previously
$\langle X, Y \rangle : XorY$	It becomes a part of message transmission $XorY$
$\langle X \rangle_Y$	X is aggregated with the message Y
$P \overset{K}{\leftrightarrow} Q$	K is a secret-key parameter likely to-be shared between P and Q
$P \overset{x}{\leftrightarrow} Q$	x is a secret key parameter known to the communication parties to provide trustworthiness
${}^{P}/_{Q}$:	Assume that if $\langle P \rangle$ is true then $\langle Q \rangle$ subsequently appeals to be true
$P \lhd C(X)$	P assures C, only if X is transmitted over communication channel C, which can be positively observed by P. Note. P should be a channel writer to read the message transmission $\langle X \rangle$
$P \lhd C\|X$	P assures C, only if X is transmitted over communication channel C, which P receives positively

$$\text{Step2}: \; U_{\text{ser}} \lhd \left\langle \left\{ \begin{array}{c} T_b(x) \quad \bmod p \\ \rightarrow \\ \text{DDHP} \langle \text{Public} \rangle \end{array} \right. R_{\text{S}}, (H(I_{\text{d}} \parallel U_{\text{id}} \parallel h(P_{\text{wd}} \parallel t) \parallel \text{TS}_1), \text{TS}_2)_\lambda, \text{TS}_2 \right\rangle$$

Rule of inference using BAN logic

A different set of inference rules using BAN logic is listed in below to derive the security robustness of the proposed S-USI scheme.

⟨Interpretation Rule⟩

I_{R1} : $\frac{P \lhd C(X), P \in r(C)}{P \equiv (P \lhd X | C), P \lhd X}$, if ⟨$P$⟩ obtains to read ⟨$X$⟩ through a wireless communication channel ⟨C⟩, then ⟨P⟩ ascertains that ⟨X⟩ has reached onto ⟨C⟩ to claim that ⟨P⟩ perceives ⟨X⟩.

I_{R2} : $\frac{P \lhd (X,Y)}{(P \lhd X)(P \lhd Y)}$, if ⟨$P$⟩ persuades a hybrid message transmission ⟨X, Y⟩, then ⟨P⟩ assures to separate the transmission ⟨X⟩ and ⟨Y⟩.

I_{R3} : $\frac{P \equiv \langle w(C) = \{P,Q\} \rangle}{P \equiv (P \lhd X | C) \rightarrow Q | \sim X}$, if ⟨$P$⟩ ascertains that ⟨$C$⟩ may only be known to ⟨$P$⟩ and ⟨$Q$⟩, then ⟨$P$⟩ assures that if ⟨$P$⟩ obtains ⟨$X$⟩ over a communication channel ⟨X⟩, then ⟨Q⟩ is said to know ⟨X⟩.

I_{R4} : $\frac{P \equiv \langle Q | \sim (X,Y) \rangle}{P \equiv (Q | \sim X), P \equiv (Q | \sim Y)}$, if ⟨$P$⟩ ascertains that ⟨$Q$⟩ is known to have a hybrid message ⟨X, Y⟩, then ⟨P⟩ assures that ⟨Q⟩ indicate a separation of ⟨X⟩ and ⟨Y⟩.

I_{R5} : $\frac{\left\langle P \equiv \xrightarrow[\text{DDHP} \langle \text{Secret} \rangle]{a} \right\rangle P, \left\langle P \equiv \xrightarrow[\text{DDHP} \langle \text{Public} \rangle]{T_b(x) \bmod p} \right\rangle Q}{\left\langle P \equiv \overset{T_{ab}(x) \bmod p}{\longleftrightarrow} Q \right\rangle}$, if ⟨$P$⟩ ascertains that ⟨$a$⟩ is said to be an extended Chebyshev chaotic-map based decisional Diffie Hellman ⟨Secret⟩ and $T_a(x) \bmod p$ is the extended Chebyshev chaotic-map based decisional Diffie Hellman ⟨Component⟩ from ⟨Secret⟩, then $T_{ab}(x) \bmod p$ is a symmetric key encryption technique to share between the communication parties i.e. P and Q.

⟨*A Rule of Key Freshness*⟩

I_{R6} : $\frac{P | \equiv \# X}{P | \equiv \# \langle X,Y \rangle}$, if P ascertains that a part of message transmission ⟨X⟩ is fresh, then it is assumed that the complete data message ⟨X, Y⟩ to provide a rule of key freshness.

I_{R7} : $\frac{P \equiv (Q | \sim X) P \equiv \#(X)}{P \equiv (Q | \sim X)}$, if P ascertains that Q obtains X and also believes X to gain a factor of key freshness, then P assures that Q has acquired the information of X.

⟨A *Rule of Rationality*⟩

I_{R8} : $\frac{P \equiv (\emptyset_1 - \emptyset_2) P \equiv \emptyset_1}{P \equiv \emptyset_2}$, if P assures that $\emptyset_1$ entails $\emptyset_2$ and P assures that $\emptyset_1$ is true, then P be certain of $\emptyset_2$ is true.

Initial BAN Logic Assumption

The following assumptions are made to analyze and prove the mutual authentication property of the proposed S-USI scheme.

$\langle A \rangle_1$: $A \in r \left\langle C_{A,B} \right\rangle$: A may read the messages through channel reader $C_{A,B}$

$\langle A \rangle_2$: $A \equiv (w \left\langle C_{A,B} \right\rangle = \langle A, B \rangle)$ =: A ascertains that A and B may write the messages through channel writer $C_{A,B}$

$\langle A \rangle_3$: $A \equiv (B \parallel\sim \emptyset \rightarrow \emptyset)$: A ascertains that B can only perceive whether the transmission is trustworthy or not.

$\langle A \rangle_4$: $A \equiv\neq \langle N_A \rangle$: A ascertains key freshness of $\langle N_A \rangle$

$\langle A \rangle_5$: $A \equiv \frac{a}{\text{DDHP} \langle \text{Secret} \rangle} \langle A \rangle$: A ascertains that a parameter ⟨a⟩ is chosen the extended Chebyshev chaotic-map based decisional Diffie Hellman problem to prove its secrecy.

Security goals

The following goals are considered to validate the mutual authentication property of the proposed S-USI scheme.

Goal_1 : $U_{\text{ser}} \equiv U_{\text{ser}} \overset{T_{ab}(x) \bmod p}{\longleftrightarrow} R_{\text{S}}$: U_{ser} ascertains that $\lambda = T_{ab}(x) \bmod p$ is a symmetric key encryption technique to share between the communication parties i.e. U_{ser} and R_{S}.

Goal_2 : $R_{\text{S}} \equiv U_{\text{ser}} \overset{T_{ab}(x) \bmod p}{\longleftrightarrow} R_{\text{S}}$: R_{S} ascertains that $\lambda = T_{ab}(x) \bmod p$ is a symmetric key encryption technique to share between the communication parties i.e. U_{ser} and R_{S}.

Goal_3 : $U_{\text{ser}} \equiv R_{\text{S}} \equiv U_{\text{ser}} \overset{T_{ab}(x) \bmod p}{\longleftrightarrow} R_{\text{S}}$: U_{ser} ascertains that R_{S} is agreed with $\lambda = T_{ab}(x) \bmod p$ as a symmetric key encryption technique to share between the communication parties i.e. U_{ser} and R_{S}.

Goal_4 : $R_{\text{S}} \equiv U_{\text{ser}} \equiv U_{\text{ser}} \overset{T_{ab}(x) \bmod p}{\longleftrightarrow} R_{\text{S}}$: Remote server R_{S} ascertains that R_{S} is agreed with $\lambda = T_{ab}(x) \bmod p$ as a symmetric key encryption technique to share between the communication parties i.e. U_{ser} and R_{S}.

To accomplish $\langle \text{Goal} \rangle_1$, the below analysis is made:

$$U_{\text{ser}} \equiv \xrightarrow[\text{DDHP} \langle \text{Secret} \rangle]{a} U_{\text{ser}} \tag{5}$$

$$\text{and } U_{\text{ser}} \equiv \xrightarrow[\text{DDHP} \langle \text{Secret} \rangle]{T_a(x) \bmod p} U_{\text{ser}}. \tag{6}$$

The Eqs. (5) and (6) should adhere owing to Interpretation Rule I_{R3} and BAN Logic Assumption $\langle A \rangle_5$. To strengthen security efficiency, the Eq. (6) has:

$$U_{\mathrm{ser}} \equiv \left(R_{\mathrm{S}} \mid\mid\!\sim \xrightarrow[\text{DDHP}\ \langle\text{public}\rangle]{T_b(x)\ \mathrm{mod}\ p} R_{\mathrm{S}}, \left(H\left(I_{\mathrm{d}} \parallel U_{\mathrm{id}} \parallel h\left(P_{\mathrm{wd}} \parallel t\right) \parallel \mathrm{TS}_1\right),\ \mathrm{TS}_2\right)_{\lambda}, \mathrm{TS}_2 \xrightarrow[\text{DDHP}\ \langle\text{public}\rangle]{T_b(x)\ \mathrm{mod}\ p} R_{\mathrm{S}} \right) \tag{7}$$

$$\text{and } U_{\mathrm{ser}} \equiv \left(R_{\mathrm{S}} \mid\mid\!\sim \xrightarrow[\text{DDHP}\ \langle\text{publicpublic}\rangle]{T_b(x)\ \mathrm{mod}\ p} R_{\mathrm{S}} \right) \tag{8}$$

The Eqs. (7) and (8) should adhere owing to BAN Logic Assumption $\langle A \rangle_3$ and Rule of Rationality I_{R8}. To extend the robustness of the proposed S-USI scheme, the Eq. (8) has:

$$U_{\mathrm{ser}} \equiv \#\left(\xrightarrow[\text{DDHP}\ \langle\text{public}\rangle]{T_b(x)\ \mathrm{mod}\ p} R_{\mathrm{S}} \right) \tag{9}$$

The Eq. (9) holds because of A Rule of Key Freshness $\langle I_{R6}, I_{R7} \rangle$ and BAN Logic Assumption $\langle A \rangle_4$. It has:

$$U_{\mathrm{ser}} \in r(C_{R_{\mathrm{S}},U_{\mathrm{ser}}}) \tag{10}$$

$$U_{\mathrm{ser}} \equiv (w\left\langle r(C_{R_{\mathrm{S}},U_{\mathrm{ser}}})\right\rangle = \left\{U_{\mathrm{ser}}, R_{\mathrm{S}}\right\}) \tag{11}$$

$$\text{and } U_{\mathrm{ser}} \equiv \lhd C_{R_S,U_{\mathrm{ser}}}\left(\xrightarrow[\text{DDHP}\ \langle\text{public}\rangle]{T_b(x)\ \mathrm{mod}\ p} R_{\mathrm{S}} \right) \tag{12}$$

The Eqs. (10), (11) and (12) hold owing to Interpretation Rule I_{R1}, I_{R2} and I_{R3} and BAN Logic Assumption $\langle A \rangle_1$ and $\langle A \rangle_2$. Using Interpretation Rule I_{R5}, the proposed S-USI scheme realizes:

$$\mathrm{Goal}_1\ :\ U_{\mathrm{ser}} \equiv \left(U_{\mathrm{ser}} \overset{T_{ab}(x)\ \mathrm{mod}\ p}{\underset{\text{DDHP}\ \langle\text{public}\rangle}{\longleftrightarrow}} R_{\mathrm{S}} \right).$$

Correspondingly, the proposed S-USI scheme derives: $\mathrm{Goal}_2\ :\ R_{\mathrm{S}} \equiv \left(U_{\mathrm{ser}} \overset{T_{ab}(x)\ \mathrm{mod}\ p}{\underset{\text{DDHP}\ \langle\text{public}\rangle}{\longleftrightarrow}} R_{\mathrm{S}} \right)$ to satisfy its conditional derivation with $\langle \mathrm{Goal} \rangle_1$. To execute the security goal Goal_3, it has:

$$U_{\mathrm{ser}} \equiv \left(R_{\mathrm{S}} \mid\mid\!\sim \left(U_{\mathrm{ser}} \overset{T_{ab}(x)\ mod\ p}{\underset{\text{DDHP}\langle\text{public}\rangle}{\longleftrightarrow}} R_{\mathrm{S}} \right) \to \left(R_{\mathrm{S}} \equiv \left(U_{\mathrm{ser}} \overset{T_{ab}(x)\ \mathrm{mod}\ p}{\underset{\text{DDHP}\ \langle\text{public}\rangle}{\longleftrightarrow}} R_{\mathrm{S}} \right) \right) \right) \Big), \tag{13}$$

$$U_{\mathrm{ser}} \equiv \left(R_{\mathrm{S}} \mid\mid\!\sim\ U_{\mathrm{ser}} \overset{T_{ab}(x)\ \mathrm{mod}\ p}{\underset{\text{DDHP}\langle\text{public}\rangle}{\longleftrightarrow}} R_{\mathrm{S}} \right). \tag{14}$$

The Eqs. (13) and (14) hold owing to the Rule of Rationality I_{R8} and BAN Logic Assumption $\langle A \rangle_3$. To accomplish the security goal, the Eq. (14) has:

$$U_{\mathrm{ser}} \equiv \left(R_{\mathrm{S}} \mid\ \sim\ U_{\mathrm{ser}} \overset{T_{ab}(x)\ \mathrm{mod}\ p}{\underset{\text{DDHP}\ \langle\text{public}\rangle}{\longleftrightarrow}} R_{\mathrm{S}} \right), \tag{15}$$

$$\text{and } U_{\mathrm{ser}} \equiv \#\left(U_{\mathrm{ser}} \overset{T_{ab}(x)\ \mathrm{mod}\ p}{\underset{\text{DDHP}\langle\text{public}\rangle}{\longleftrightarrow}} R_{\mathrm{S}} \right). \tag{16}$$

The Eqs. (15) and (16) hold owing to A Rule of Key Freshness $\langle I_{R6}, I_{R7} \rangle$ and BAN Logic Assumption $\langle A \rangle_4$. To achieve the Eq. (16), it has:

$$U_{\mathrm{ser}} \in r(C_{R_{\mathrm{S}},U_{\mathrm{ser}}}), \tag{17}$$

$$U_{\mathrm{ser}} \equiv (\left\langle r(C_{R_{\mathrm{S}},U_{\mathrm{ser}}})\right\rangle = \left\{U_{\mathrm{ser}}, R_{\mathrm{S}}\right\}), \tag{18}$$

$$\text{and } U_{\mathrm{ser}} \lhd C_{R_{\mathrm{S}},U_{\mathrm{ser}}}\left(\xrightarrow[\text{DDHP}\ \langle\text{public}\rangle]{T_{ab}(x)\ \mathrm{mod}\ p} R_{\mathrm{S}} \right). \tag{19}$$

The Eqs. (17), (18) and (19) hold owing to Interpretation Rule I_{R1}, I_{R2}, I_{R5} and BAN Logic Assumption $\langle A \rangle_1$, $\langle A \rangle_2$ and $\langle A \rangle_5$. Therefore, the proposed S-USI scheme has:

$$\mathrm{Goal}_3\ :\ U_{\mathrm{ser}} \equiv R_{\mathrm{S}} \equiv U_{\mathrm{ser}} \xrightarrow[\text{DDHP}\langle\text{public}\rangle]{T_{ab}(x)\ \ \mathrm{mod}\ \ p} R_{\mathrm{S}}.$$

Similarly, the proposed S-USI scheme derives $\langle \mathrm{Goal} \rangle_3$ to satisfy its conditional derivation with $\langle \mathrm{Goal} \rangle_3$. To execute the security goal Goal_4, it has:

$$\mathrm{Goal}_4\ :\ R_{\mathrm{S}} \equiv U_{\mathrm{ser}} \equiv U_{\mathrm{ser}} \xrightarrow[\text{DDHP}\langle\text{public}\rangle]{T_{ab}(x)\ \ \mathrm{mod}\ \ p} R_{\mathrm{S}}.$$

Eventually, the proposed S-USI scheme gains the $\mathrm{Goal}_1, \mathrm{Goal}_2, \mathrm{Goal}_3$ and Goal_4 to satisfy the property of mutual authentication between U_{ser} and R_{S}.

Comparison of communication and storage cost

Assume that length of the identity of U_{sr} U_{id} and password P_{wd}, random-integer and hash-function are set to 160 bits, whereas the elliptic-curve considers 320 bits and the symmetric key encryption/decryption carries a size of 512 bits [75]. In the S-USI scheme, three message rounds are considered such as $M_{\mathrm{sg1}} = \langle P_1, P_2, \mathrm{TS}_1 \rangle$, $M_{\mathrm{sg2}} = \langle Q_1, Q_2, \mathrm{TS}_2 \rangle$ and $\langle R, H \rangle$ to transmit between U_{ser} and R_{S}. Thus, the total communication cost of the proposed S-USI scheme is carefully computed: $\langle 320 + 320 + 160 + 160 \rangle = 960$ bits in comparison with other existing authentication schemes

Table 5 Comparison of proposed S-USI and other related schemes with communication, computation, and storage cost

Properties schemes	RP	LAP	TC	CC (bits)	SC (bits)	ET (s)
Nikooghadam et al. [64]	$2\mathrm{ET}_H + 1\mathrm{ET}_{\mathrm{SED}}$	$6\mathrm{ET}_H + 6\mathrm{ET}_{\mathrm{SED}}$	$8\mathrm{ET}_H + 7\mathrm{ET}_{\mathrm{SED}}$	1728	1504	0.0649
Chaudhry et al. [65]	$4\mathrm{ET}_H + 2\mathrm{ET}_{\mathrm{SED}} + 1\mathrm{ET}_{\mathrm{DM}}$	$14ET_H + 6ET_{SED} + 7ET_{DM}$	$18\mathrm{ET}_H + 8\mathrm{ET}_{\mathrm{SED}} + 8\mathrm{ET}_{\mathrm{DM}}$	1344	1696	0.5832
Arshad et al. [66]	$3\mathrm{ET}_H$	$14\mathrm{ET}_H + 6\mathrm{ET}_{\mathrm{DM}}$	$17\mathrm{ET}_H + 6\mathrm{ET}_{\mathrm{DM}}$	1312	1120	0.3869
Lu et al. [67]	$3\mathrm{ET}_H$	$11\mathrm{ET}_H + 4\mathrm{ET}_{\mathrm{DM}}$	$14\mathrm{ET}_H + 4\mathrm{ET}_{\mathrm{DM}}$	1376	800	0.2593
Amin and Biswas [69]	$3\mathrm{ET}_H + 1\mathrm{ET}_{\mathrm{DM}}$	$9\mathrm{ET}_H + 5\mathrm{ET}_{\mathrm{DM}} + 2\mathrm{ET}_{\mathrm{SED}}$	$12\mathrm{ET}_H + 6\mathrm{ET}_{\mathrm{DM}} + 2\mathrm{ET}_{\mathrm{SED}}$	1984	1472	0.3474
Chandrakar et al. [75]	$6\mathrm{ET}_H + 4\mathrm{ET}_{\mathrm{DM}}$	$18\mathrm{ET}_H + 8\mathrm{ET}_{\mathrm{DM}}$	$24\mathrm{ET}_H + 12\mathrm{ET}_{\mathrm{DM}}$	1120	1440	0.7689
Proposed S-USI scheme	$3\mathrm{ET}_H + 2\mathrm{ET}_{\mathrm{ME}}$	$8\mathrm{ET}_H + 1\mathrm{ET}_{\mathrm{ME}} + 1\mathrm{ET}_{\mathrm{SED}}$	$11\mathrm{ET}_H + 3\mathrm{ET}_{\mathrm{ME}} + 1\mathrm{ET}_{\mathrm{SED}}$	960	896	0.0689

RP registration phase, *LAP* login and authentication phase, *TC* total cost, *CC* communication cost, *SC* storage cost, *ET* execution time

[64–67, 69, 75] such as 1728 bits, 1344 bits, 1312 bits, 1376 bits, 1984 bits, and 1120 bits, respectively. Moreover, as the smartcard is highly expensive, the storage capacity of the device is restricted to reduce the storage overheads. In the proposed S-USI scheme, the storage parameters are $\langle R^{\mathrm{new}}, h(.), E_k(.), x, T_r(x)\rangle$, which has a total cost $\langle 160 + 160 + 256 + 160 + 160\rangle = 896$ bits. However, the other existing authentication schemes [64–67, 69, 75] consume the storage cost sizes such as 1504 bits, 1696 bits, 1120 bits, 800 bits, 1472 bits, and 1440 bits correspondingly shown in Table 5.

From Table 5, the performance analysis can also be observed in terms of the execution time of hash operation $\langle \mathrm{ET}_H\rangle$, chaotic-map operation $\langle \mathrm{ET}_{\mathrm{CM}}\rangle$, symmetric encryption/decryption $\langle \mathrm{ET}_{\mathrm{SED}}\rangle$, squaring operation $\langle \mathrm{ET}_{\mathrm{SO}}\rangle$, square-root solving operation $\langle \mathrm{ET}_{\mathrm{SRS}}\rangle$, division/multiplication operation $\langle \mathrm{ET}_{\mathrm{DM}}\rangle$ and modular-exponential computation $\langle \mathrm{ET}_{\mathrm{ME}}\rangle$ in comparison with other existing schemes [64–67, 69, 75].

While comparing the computation costs of various system phases, it is observed that the proposed S-USI scheme consumes $3\mathrm{ET}_H + 2\mathrm{ET}_{\mathrm{ME}}$ for registration and $8\mathrm{ET}_H + 1\mathrm{ET}_{\mathrm{ME}} + 1\mathrm{ET}_{\mathrm{SED}}$ for login and authentication, whereas Nikooghadam et al. [64] have $2\mathrm{ET}_H + 1\mathrm{ET}_{\mathrm{SED}}$ for registration and $6\mathrm{ET}_H + 6\mathrm{ET}_{\mathrm{SED}}$ for login and authentication; Chaudhry et al. [65] acquire $4\mathrm{ET}_H + 2\mathrm{ET}_{\mathrm{SED}} + 1\mathrm{ET}_{\mathrm{DM}}$ for registration and $14\mathrm{ET}_H + 6\mathrm{ET}_{\mathrm{SED}} + 7\mathrm{ET}_{\mathrm{DM}}$ for login and authentication; Arshad et al. [66] hold $3\mathrm{ET}_H$ for registration and $14\mathrm{ET}_H + 6\mathrm{ET}_{\mathrm{DM}}$ for login and authentication; Lu et al. [67] possess $3\mathrm{ET}_H$ for registration and $11\mathrm{ET}_H + 4\mathrm{ET}_{\mathrm{DM}}$ for login and authentication; Amin and Biswas [69] experience $3\mathrm{ET}_H + 1\mathrm{ET}_{\mathrm{DM}}$ for registration and $9\mathrm{ET}_H + 5\mathrm{ET}_{\mathrm{DM}} + 2\mathrm{ET}_{\mathrm{SED}}$ for login and authentication; Chandrakar et al. [75] have $6\mathrm{ET}_H + 4\mathrm{ET}_{\mathrm{DM}}$ for registration and $18\mathrm{ET}_H + 8\mathrm{ET}_{\mathrm{DM}}$ for login and authentication. The above analysis proves that the proposed S-USI scheme uses less computation cost over the execution of registration, login, and authentication phases as compared to other existing schemes [64–67, 69, 75] except Nikooghadam et al. [64]. However, Nikooghadam et al. [64] could not withstand most of the vulnerable attacks shown in Table 2. Therefore, the other existing schemes [64–67, 69, 75] cannot be recommended for cloud-based TMIS as they could not be resistant to various susceptibilities.

Four cryptographic operations such as $\langle \mathrm{ET}_H\rangle, \langle \mathrm{ET}_{\mathrm{SED}}\rangle, \langle \mathrm{ET}_{\mathrm{DM}}\rangle$ and $\langle \mathrm{ET}_{\mathrm{ME}}\rangle$ are considered to determine the execution time of authentication protocol. To effectively analyze the execution cost, the system login and authentication are deliberately chosen as the communication happens only between U_{ser} and R_{S} to-do any intercommunication. As referred to [26], the approximate execution time of the cryptographic operation was done in the configuration of Intel® Core ™ i5-7200 CPU @ 2.7 GHz, 16.0 GB RAM, and OS: Win 10 64-bit along with Visual Studio 2008 software using MIRACL C/C++ library. Also, the algorithms such 1024-bit Rivest-Shamir-Adleman (RSA) algorithm, 320-bits elliptic-curve (EC) cryptosystem, 128-bit advanced-encryption standard (AES), and 160 -bit secure-hash algorithm 1 (SHA-1) were employed to experiment the given assumption time that is as follows: $\mathrm{ET_H} \approx 0.0004$ ms, $\mathrm{ET}_{\mathrm{SED}} \approx 0.1303$ ms, $\mathrm{ET}_{\mathrm{DM}} \approx 1.8269$ ms and $\mathrm{ET}_{\mathrm{ME}} \approx 1.6003$ ms in the given order [8]. From Table 3, the estimated execution time of the proposed S-USI scheme and other related schemes such as Nikooghadam et al. [64], Chaudhry et al. [65], Arshad et al. [66], Lu et al. [67], Amin and Biswas [69], and Chandrakar et al. [75] were carefully examined to determine the execution time. The result of the proposed S-USI was 0.0689 ms, whereas the other related schemes were 0.0649 s, 0.5832 s, 0.3869 s, 0.2593 s, 0.3474 s, and 0.7689 s respectively. It is also shown that the proposed S-USI scheme is minimum in comparison with other related authentication except for Nikooghadam et al. However, Nikooghadam et al. [64] could not be much reliable for cloud-based TMIS as it was dissatisfying most of the security vulnerabilities such as denial-of-service, privileged-insider, user anonymity, identity protection, forgery, masquerade and user impersonation attack.

Discussions

In the past, several user authentication schemes have been proposed for the support of system efficiencies such as communication, computation, and storage. Specifically, in sensor technologies, the specific area of key agreement (KA) schemes [61–68] has often been chosen, though they are not suitable to provide better energy utilization and environment adaptability. In [69], the KA scheme is generally classified into traditional, physiological value, secret-key generation, and hybrid-key that tries to provide a secret session-key to authorize the data transmission between the real-time entities. The hybrid-key authentication scheme incorporates either traditional, physiological value or secret-key generation to employ symmetric or public-key cryptosystems to minimize the computation, communication, or storage cost. However, the above classification techniques are still addressing the challenges of security and privacy as the communication between the sensor network and the device is typically taking place over insecure public networks.

Generally speaking, key agreement using elliptic-curve cryptography becomes more appealing to achieve less computation overhead. However, it is still computationally expensive [57]. The traditional scheme literally suffers from unresponsive network change, whereby the performance efficiency would be deliberately degraded. Fortunately, the scheme with the pre-deployment key phase always improves communication efficiency as they use lightweight operations. In literature, various user authentication protocols have been designed for telecare medical information systems that address several challenges such as (1) most of the authentication schemes are completed relied on password and smartcard; (2) some authentication schemes could not resist identity and password-guessing attacks; (3) the majority of the schemes could not provide session key agreement and proper mutual authentication; (4) very few user authentication protocols have been verified formally using a random-oracle model, automated validation of internet security protocol and application (AVISPA), cryptographic protocol verifier known as ProVerif, and Burrows Abadi Needham (BAN) logic; (5) relatively more authentication schemes do not comply with forward secrecy; and (6) almost all the authentication scheme does not provide better performance efficiencies namely computation, communication, and storage. To resolve the above addressing issues, an authentication scheme known as single-user sign-in authentication (S-USI) mechanism is proposed i.e. specifically for cloud-based TMIS using extended Chebyshev chaotic-map based decisional Diffie Hellman problem (DDHP).

Conclusion

For cloud-based TMIS, a key element known as information security has played a significant role. To provide a corrective approach, a strategy of single-user sign-in authentication (S-USI) mechanism has been proposed using extended Chebyshev chaotic-map based decisional Diffie Hellman problem (DDHP). To meet the current demands of sensor intelligence networks, this mechanism practices on a strategy of unary-token to access the service that annuls the clock synchronization problem. As the proposed S-USI is based on DDHP, the formal and informal security analysis proves that the malicious user or any adversary cannot logically deduce any confidential parameter to derive a session-key authorized between U_{ser} and R_{S}. In addition, this proposed mechanism claims that no malicious user can forge a valid user authentication request or personate as a legitimate user as it is based on Chebyshev chaotic-map. The formal verification using AKE Session-Key Security and BAN logic demonstrates that the proposed S-USI mechanism can be resilient to various potential attacks such as replay, denial-of-service, privileged-inside, etc. Also, the comparative analysis shows that the proposed S-USI mechanism mitigates the computation, communication, and storage cost to improve the performance efficiency of pervasive services in the cloud. In the future, the proposed S-USI will be evaluated using NS-3 to analyze the quality metrics such as transmission delay, throughput rate, and routing overhead. Based on the experimental analysis, the proposed S-USI will be optimized further to meet the standard requirements of the computing paradigms. In addition, an energy consumption model will be built to make the proposed mechanism to be more dynamic in cloud-IoT environments.

Compliance with ethical standards

Conflict of interest We declare that we do not have any commercial or associative interest that represents a conflict of interest in connection with the work submitted.

References

1. Bibri SE, Krogstie J (2017) ICT of the new wave of computing for sustainable urban forms: their big data and context-aware augmented typologies and design concepts. Sustain Cities Soc 32:449–474
2. Bibri SE, Krogstie J (2017) Smart sustainable cities of the future: an extensive interdisciplinary literature review. Sustain Cities Soc 31:183–212
3. Mehmood Y, Ahmad F, Yaqoob I, Adnane A, Imran M, Guizani S (2017) Internet-of-things-based smart cities: recent advances and challenges. IEEE Commun Mag 55(9):16–24
4. Salman O, Elhajj I, Kayssi A, Chehab A (2015) Edge computing enabling the Internet of Things. In: 2015 IEEE 2nd world forum on Internet of Things (WF-IoT). IEEE, pp 603–608
5. 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
6. Fadi AT, David DB (2020) Seamless authentication: for IoT-big data technologies in smart industrial application systems. IEEE Trans Ind Informat
7. 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
8. David DB (2017) Mutual authentication scheme for multimedia medical information systems. Multimedia Tools Appl 76(8):10741–10759
9. 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 Inf 15(9):4957–4968
10. Mohammad Z, Abusukhon A, Qattam TA (2019) A survey of authenticated key agreement protocols for securing IoT. In: 2019 IEEE Jordan international joint conference on electrical engineering and information technology (JEEIT). IEEE, pp 425–430
11. Wazid M, Das AK, Hussain R, Succi G, Rodrigues JJ (2019) Authentication in cloud-driven IoT-based big data environment: survey and outlook. J Syst Arch 97:185–196
12. Jia X, He D, Kumar N, Choo KKR (2019) Authenticated key agreement scheme for fog-driven IoT healthcare system. Wirel Netw 25(8):4737–4750
13. Kumari S, Renuka K (2019) Design of a password authentication and key agreement scheme to access e-healthcare services. Wirel Pers Commun:1–19
14. Ostad-Sharif A, Abbasinezhad-Mood D, Nikooghadam M (2019) A robust and efficient ECC-based mutual authentication and session key generation scheme for healthcare applications. J Med Syst 43(1):10
15. Deebak BD, Al-Turjman F, Aloqaily M, Alfandi O (2020) IoT-BSFCAN: a smart context-aware system in IoT-Cloud using mobile-fogging. Future Gen Comput Syst
16. Jain U, Hussain M, Kakarla J (2020) Simple, secure, and lightweight mechanism for mutual authentication of nodes in tiny wireless sensor networks. Int J Commun Syst 33(9):e4384
17. Wu F, Li X, Xu L, Vijayakumar P, Kumar N (2020) A novel three-factor authentication protocol for wireless sensor networks with IoT notion. IEEE Syst J
18. Kumar D, Singh HK, Ahlawat C (2019) A secure three-factor authentication scheme for wireless sensor networks using ECC. J Discrete Math Sci Cryptogr:1–22
19. Chen Y, Ge Y, Wang Y, Zeng Z (2019) An improved three-factor user authentication and key agreement scheme for wireless medical sensor networks. IEEE Access 7:85440–85451
20. Senyo PK, Addae E, Boateng R (2018) Cloud computing research: a review of research themes, frameworks, methods and future research directions. Int J Inf Manage 38(1):128–139
21. Mell P, Grance T (2011) The NIST definition of cloud computing, special publication 800-145, Nat'l Inst. Standards and Technology
22. Senyo PK, Effah J, Addae E (2016) Preliminary insight into cloud computing adoption in a developing country. J Enterprise Inf Manag
23. Smara M, Aliouat M, Pathan ASK, Aliouat Z (2017) Acceptance test for fault detection in component-based cloud computing and systems. Future Gen Comput Syst 70:74–93
24. Zhou S, Wu L, Jin C (2017) A privacy-based SLA violation detection model for the security of cloud computing. China Commun 14(9):155–165
25. Chen CH, Lin JW, Kuo SY (2015) MapReduce scheduling for deadline-constrained jobs in heterogeneous cloud computing systems. IEEE Trans Cloud Comput 6(1):127–140
26. 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
27. Alam MM, Malik H, Khan MI, Pardy T, Kuusik A, Le Moullec Y (2018) A survey on the roles of communication technologies in IoT-based personalized healthcare applications. IEEE Access 6:36611–36631
28. Baali H, Djelouat H, Amira A, Bensaali F (2017) Empowering technology enabled care using IoT and smart devices: a review. IEEE Sens J 18(5):1790–1809
29. Chaudhari DA, Umamaheswari E (2018) Survey on data management for healthcare using internet of things. In: 2018 Fourth international conference on computing communication control and automation (ICCUBEA). IEEE, pp 1–7
30. Suguna M, Ramalakshmi MG, Cynthia J, Prakash D (2018) A survey on cloud and Internet of Things based healthcare diagnosis. In: 2018 4th international conference on computing communication and automation (ICCCA). IEEE, pp 1–4
31. Gandhi DA, Ghosal M (2018) Intelligent healthcare using IoT: a extensive survey. In: 2018 Second international conference on inventive communication and computational technologies (ICICCT). IEEE, pp 800–802
32. Khan I, Amaro AC, Oliveira L (2019) IoT-based systems for improving older adults' wellbeing: a systematic review. In: 2019 14th Iberian conference on information systems and technologies (CISTI). IEEE, pp 1–6
33. Darshan KR, Anandakumar KR (2015). A comprehensive review on usage of Internet of Things (IoT) in healthcare system. In: 2015 International conference on emerging research in electronics, computer science and technology (ICERECT). IEEE, pp 132–136
34. Deebak BD, Al-Turjman F (2020) Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things. IEEE J Select Areas Commun
35. Deebak BD (2020) Lightweight authentication and key management in mobile-sink for smart IoT-assisted systems. Sustain Cities Soc 63:102416
36. Deebak BD, Al-Turjman F, Mostarda L (2020) Seamless secure anonymous authentication for cloud-based mobile edge computing. Comput Electr Eng 87:106782
37. Ostad-Sharif A, Abbasinezhad-Mood D, Nikooghadam M (2019) An enhanced anonymous and unlinkable user authentication and key agreement protocol for TMIS by utilization of ECC. Int J Commun Syst 32(5):e3913
38. Guo X, Zhang J (2010) Secure group key agreement protocol based on chaotic hash. Inf Sci 180:4069–4074
39. Xiao D, Liao X, Deng S (2007) A novel key agreement protocol based on chaotic maps. Inf Sci 177:1136–1142

40. Xue K, Hong P (2012) Security improvement on an anonymous key agreement protocol based on chaotic maps. Commun Nonlinear Sci Numer Simul 17:2969–2977
41. Tan Z (2013) A chaotic maps-based authenticated key agreement protocol with strong anonymity. Nonlinear Dyn 72:311–320
42. Guo C, Chang C-C (2013) Chaotic maps-based password-authenticated key agreement using smart cards. Commun Nonlinear Sci Numer Simul 18:1433–1440
43. Hao X, Wang J, Yang Q, Yan X, Li P (2013) A chaotic map-based authentication scheme for telecare medicine information systems. J Med Syst 37
44. Jiang Q, Ma J, Lu X, Tian Y (2014) Robust chaotic map-based authentication and key agreement scheme with strong anonymity for telecare medicine information systems. J Med Syst 38:12
45. Lee T-F (2013) An efficient chaotic maps-based authentication and key agreement scheme using smartcards for telecare medicine information systems. J Med Syst 37:9985
46. Mishra D, Srinivas J, Mukhopadhyay S (2014) A secure and efficient chaotic mapbased authenticated key agreement scheme for telecare medicine information systems. J Med Syst 38:1–10
47. Li C-T, Lee C-C, Weng C-Y (2014) A secure chaotic maps and smart cards based password authentication and key agreement scheme with user anonymity for telecare medicine information systems. J Med Syst 38:1–11
48. Wang Z, Huo Z, Shi W (2015) A dynamic identity based authentication scheme using chaotic maps for telecare medicine information systems. J Med Syst 39:1–8
49. Bergamo P, D'Arco P, De Santis A, Kocarev L (2005) Security of public-key cryptosystems based on chebyshev polynomials. IEEE Trans Circuits Syst I Regul Pap 52:1382–1393
50. Lee T-F (2015) Enhancing the security of password authenticated key agreement protocols based on chaotic maps. Inform Sci 290:63–71
51. Islam S, Obaidat MS, Amin R (2016) An anonymous and provably secure authentication scheme for mobile user. Int J Commun Syst 29:1529–1544
52. Lin H-Y (2014) Chaotic map based mobile dynamic id authenticated key agreement scheme. Wirel Pers Commun 78:1487–1494
53. Liu Y, Xue K (2016) An improved secure and efficient password and chaos-based two-party key agreement protocol. Nonlinear Dyn 84:549–557
54. Madhusudhan R, Nayak CS (2019) A robust authentication scheme for telecare medical information systems. Multimedia Tools Appl 78(11):15255–15273
55. Biswas A, Roy A (2019) A study on Dynamic ID based user authentication system using smart card. AJCT 5(2)
56. Chen CL, Deng YY, Weng W, Chen CH, Chiu YJ, Wu CM (2020) A traceable and privacy-preserving authentication for UAV communication control system. Electronics 9(1):62
57. Yao H, Wang C, Fu X, Liu C, Wu B, Li F (2019) A privacy-preserving RLWE-based remote biometric authentication scheme for single and multi-server environments. IEEE Access 7:109597–109611
58. Sarkar BK (2017) Big data for secure healthcare system: a conceptual design. Complex Intell Syst 3(2):133–151
59. Gomathi P, Baskar S, Shakeel PM Concurrent service access and management framework for user-centric future internet of things in smart cities
60. Mahmoud NM, Fouad H, Soliman AM (2020) Smart healthcare solutions using the internet of medical things for hand gesture recognition system. Complex Intell Syst:1–12
61. Zhou L, Li X, Yeh KH, Su C, Chiu W (2019) Lightweight IoT-based authentication scheme in cloud computing circumstance. Future Gen Comput Syst 91:244–251
62. Pak K, Pak S, Ho C, Pak M, Hwang C (2019) Anonymity preserving and round effective three-party authentication key exchange protocol based on chaotic maps. PloS One 14(3):e0213976
63. Zhang L (2008) Cryptanalysis of the public key encryption based on multiple chaotic systems. Chaos Solitons Fract 37(3):669–674
64. Nikooghadam M, Jahantigh R, Arshad H (2017) A lightweight authentication and key agreement protocol preserving user anonymity. Multimedia Tools Appl 76(11):13401–13423
65. Chaudhry SA, Naqvi H, Shon T, Sher M, Farash MS (2015) Cryptanalysis and improvement of an improved two factor authentication protocol for telecare medicine information systems. J Med Syst 39(6):1–11
66. Arshad H, Teymoori V, Nikooghadam M, Abbassi H (2015) On the security of a two-factor authentication and key agreement scheme for telecare medicine information systems. J Med Syst 39(8):1–10
67. Lu Y, Li L, Peng H, Yang Y (2015) An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem. J Med Syst 39(3):1–8
68. Wu F, Xu L, Kumari S, Li X, Das AK, Khan MK, Karuppiah M, Baliyan R (2016) A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks. Secur Commun Netw 9:3527–3542
69. Amin R, Biswas GP (2015) A secure three-factor user authentication and key agreement protocol for TMIS with user anonymity. J Med Syst 39(8):1–19
70. Abdalla M, Fouque PA, Pointcheval D (2005) Password-based authenticated key exchange in the three-party setting. In: Proc. of public key cryptography—PKC 2005, lecture notes in computer science 3386, pp 65–84
71. Abdalla M, Pointcheval D (2005) Simple password-based authenticated key protocols, topics in cryptology—CT-RSA. Lect Notes Comput Sci 3376:191–208
72. Lee CC, Hsu CW (2013) A secure biometric-based remote user authentication with key agreement scheme using extended chaotic maps. Nonlinear Dyn 71:201–211
73. Chandrakar P, Om H (2016) Cryptanalysis and extended three-factor remote user authentication scheme in multi-server environment. Arab J Sci Eng 42(2):765–786
74. Bellare M, Pointcheval D, Rogaway P (2000) Authenticated key exchange secure against dictionary attacks. In: Proc. of Advances in Cryptology—Eurocrypt 2000, lecture notes in computer science 1807, pp 139–155
75. Chandrakar P, Om H (2018) An extended ECC-based anonymity-preserving 3-factor remote authentication scheme usable in TMIS. Int J Commun Syst:e3540
76. Burrows M, Abadi M, Needham R (1990) A logic of authentication. ACM Trans Comput Syst 8(1):18–36
77. Buttyan L, Hubaux JP (2007) Security and cooperation in wireless networks: thwarting malicious and selfish behavior in the age of ubiquitous computing. Cambridge University Press, Cambridge

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