Journal of Engineering and Applied Science

RESEARCH Open Access

Anonymous and robust biometric authentication scheme for secure social IoT healthcare applications

T. Arpitha[1*], Dharamendra Chouhan[1] and J. Shreyas[2]

*Correspondence:
arpitha811@gmail.com

[1] Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bengaluru, India
[2] Department of Information Technology, Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, Manipal, India

Abstract

In the era of rapid technological advancement, the Internet of Things (IoT) has revolutionised healthcare through systems like the Telecare Medicine Information System (TMIS), designed to streamline patient-doctor interactions and enhance medical treatment. However, the transmission of sensitive patient data over inherently insecure Internet channels exposes it to a spectrum of security risks. Protecting patient medical privacy and ensuring system reliability necessitate mutual authentication between both patients and medical servers. TMIS relies on robust authentication mechanisms, and combining passwords and smart cards has been a recognised approach for mutual authentication. This research introduces an innovative three-factor authentication technique with perfect forward secrecy by leveraging the power of Elliptic Curve Cryptography (ECC) in tandem with smart cards. Additionally, we have incorporated biometric authentication with a Fuzzy Extractor technology to enhance the security and reliability of the system, setting a new standard for user authentication within the realm of Social IoT healthcare. The use of ECC in the method is justified due to its compact key size and robust security measures, making the solution both efficient and secure. The proposed method safeguards user privacy by permitting registered users to change their passwords without divulging their identity to the server. The Burrows–Abadi–Needham logic (also known as the BAN logic) serves as a proof-of-concept for the proposed scheme's security. Our system provides privacy protection along with mutual authentication and session key negotiation at a considerably low computation cost and communication cost of up to 71.03% compared to the other four relevant techniques, making it more useful in real-world scenarios.

Keywords: User authentication, User anonymity, IoT, Key agreement, Healthcare, Elliptic curve cryptography, BAN logic

Introduction

With technology changing quickly and Internet of Things (IoT) gadgets used by a lot of people, the healthcare business has changed in big ways. E-healthcare apps, which allow for online tracking, diagnosis, and treatment, are starting to look like a good way to make healthcare services more accessible and improve quality. However, ensuring that users' health data is private and safe in an open route is subject to both passive and

Springer Open

active attacks, and it remains a major worry. In the context of Social IoT, where interconnected devices and users collaborate and share information, secure anonymous mutual authentication is essential in safeguarding the privacy and integrity of e-healthcare services. Traditional authentication mechanisms, such as username and password combinations, are no longer sufficient in the face of increasingly sophisticated cyber threats. Therefore, the development of robust authentication schemes that incorporate multiple factors while preserving user anonymity is imperative.

Authentication protocols are crucial cryptographic security mechanisms used to validate users and establish shared encryption keys, playing a vital role in securing communication within the Internet of Things (IoT); however, the IoT authentication landscape faces persistent challenges concerning both security and efficiency. Despite the primary goal of enhancing security, certain IoT authentication protocols fall short due to insufficient consideration and potential design vulnerabilities. On the one hand, evolving research demands more comprehensive security requirements that many previously proposed protocols struggle to meet, while on the other hand, newly introduced "secure" protocols have, at times, revealed hidden security weaknesses upon closer examination.

Efficiency is another pivotal challenge in IoT protocol design, particularly for resource-constrained IoT environments where limited CPU, memory, and battery resources necessitate streamlined authentication schemes. Therefore, successful IoT authentication designs must not only ensure robust security but also prioritise efficiency, including reduced computational and communication overheads, to ensure practical implementation across IoT hardware. In this context, the research on practical authentication protocols recognises the paramount role of security. While some lightweight authentication schemes have proven effective against general attacks, there remains a dearth of in-depth exploration of schemes tailored for specific conditions, such as prolonged key leakage, especially in the context of the IoT, where both high computing and communication efficiency are imperative [1–7].

Motivation

The convergence of Social Internet of Things (SIoT) along with Telemedicine information systems (TMIS) has enabled the development of innovative healthcare apps that have the potential to revolutionise the field. These applications enable remote patient monitoring, enhance patient involvement, and foster collaborative treatment. However, the exchange of sensitive patient data and the interconnected nature of these systems raise significant security and privacy concerns. Ensuring the confidentiality, integrity, and availability of healthcare information is crucial to building trust and confidence among patients, healthcare providers, and other stakeholders. Traditional security mechanisms may not be sufficient to address the unique challenges posed by SIoT TMIS healthcare applications. The need for robust security solutions that can protect patient data, authenticate users, and prevent unauthorised access becomes imperative. Moreover, privacy concerns regarding the collection, storage, and transmission of personal health information require careful consideration. In this context, an ECC and Hash-based solution emerges as an appealing approach to enhance security and privacy in SIoT TMIS healthcare applications. ECC offers strong encryption and authentication capabilities, while Hash functions to ensure data integrity. By leveraging these techniques, healthcare organisations can establish a secure and private environment for data exchange, enabling efficient and reliable healthcare services while safeguarding patient information. This paper aims to explore the potential of ECC and Hash-based solutions in addressing security and privacy challenges in SIoT TMIS so healthcare providers and system designers can make informed decisions to protect healthcare applications. By understanding the benefits and implementation aspects of these techniques, sensitive patient data mitigate security risks and build resilient and trustworthy SIoT TMIS ecosystems.

Overall, the motivation behind this research is to bridge the gap between the growing importance of SIoT TMIS healthcare applications and the need for robust security measures. By exploring the potential of ECC and Hash-based solutions, this paper aims to contribute to the development of secure, privacy-enhanced, and reliable healthcare systems that can effectively serve patients, healthcare providers, and stakeholders in the digital age.

Contribution

Recently, Sahoo et al. [8] introduced a three-factor authentication scheme based on Elliptic Curve Cryptography (ECC) tailored for healthcare systems utilising Internet of Things (IoT) devices. However, their scheme falls short of ensuring user untraceability. Furthermore, it is worth noting that public-key cryptography-based methods, as mentioned earlier, exhibit certain security vulnerabilities and entail time-consuming operations. Consequently, these authentication schemes may not be well-suited for the unique demands of e-health environments. Based on the work of Sahoo et al., this paper presents an enhanced three-factor authentication protocol that can both address the shortcomings of Sahoo et al. and offer more comprehensive security in terms of perfect forward secrecy and resistance to special attacks. It also achieves lower computing overhead and communication overhead, allowing security and efficiency to coexist. Below is a summary of the paper's contributions.

1. Building on the work of Sahoo et al., a safe and effective three-factor authentication technique is suggested that offers the lowest communication and computing costs when compared to similar state-of-the-art techniques.
2. In addition to its high efficiency, the suggested technique achieves more security characteristics than current mutual authentication protocols and offers perfect forward secrecy.
3. We have incorporated biometric authentication, coupled with Fuzzy Extractor technology, which adds a layer of security that ensures the authenticity of users and protects against impersonation.
4. The scheme has undergone thorough security assessments, formally by the use of well-established BAN logic and informally, validating its robustness against potential threats. The results of our performance comparisons indicate that our scheme offers a high level of security while keeping its computation and communication overheads at an acceptable level.

The present article is organised in an orderly manner as follows: The "Related work" section offers an extensive and thorough examination of the relevant literature. The "Basic terms" section provides an overview of the fundamental prerequisites of the approach and the model used to assess potential threats. The "Problem formulation" section provides a comprehensive overview of the technique and constituent elements of the proposed secure anonymous mutually authenticating approach, which is based on a three-factor framework. The "Proposed system" section of the paper delves into the comprehensive examination of the scheme's security, including both formal and informal analyses. The "Analysis of security measures" section assesses the efficacy of the suggested methodology. In conclusion, the "Security requirement discussion" section provides a comprehensive assessment of the contributions made in this study, as well as suggested avenues for future research in the field.

Related work

The investigation of various mutual authentication techniques for TMIS has garnered the interest of several scholars. The authors have provided a range of mutual authentication mechanisms for TMIS, including password-based, smart card-based, and biometric-based strategies. These methods were based on the utilisation of RSA, chaotic map, and ECC cryptosystems. Since the beginning of the decade, many authentication and key agreement techniques [1–3] have been introduced, and it has been shown that many of these approaches are susceptible to several well-recognised security vulnerabilities.

The biometric-based authentication approach for TMIS, which depends on a hash function, was presented by Tan et al. in their paper in 2013 [4]. The individual said that their methodology demonstrates superior performance compared to established proficient systems in regard to user authentication process, key agreement effectiveness, and security. In their study, Yan et al. [5] introduced an enhanced technique and argued that Tan's approach is more prone to DoS attacks.

In the same year, Xin et al. [6] proposed an authentication approach that leverages elliptic curve cryptography to augment the efficiency and security attributes of the authentication mechanism. In a further study conducted in 2014, Islam et al. [7] identified some vulnerabilities in the technique proposed by Xu et al. [9]. Specifically, their findings revealed that the system is susceptible to replaying attacks and lacks robust authentication process, smart card revocation, and proper password reset mechanisms. In response to the limitations identified in the methodology used by Xu et al., Islam et al. put out an alternative framework. The research done by Mishra et al. [11] has shown that the system created by Yan et al. [5] has identified shortcomings in relation to user secrecy and susceptibility to guessing password. Turkanović et al. [26] introduced an innovative authentication along with a key agreement method for enhancing the security of various wireless ad hoc networks within the framework of IoT. The strategy used in their methodology integrates the usage of lightweight procedures, hash functions, and XOR operations. Additionally, it encompasses many characteristics like authentication through mutual key agreement, password modification, and dynamic node addition. The authors furthermore said that their methodology exhibits resilience against diverse challenges, concurrently reducing expenses and guaranteeing optimal performance. Moreover, Amin et al. [10] have asserted that Mishra et al.'s [11] approach exhibits vulnerabilities pertaining to system impersonation, smart card loss, and session key computation attacks.

In a research done in 2016, Farash et al. [12] revealed many security flaws inside the approach given by Turkanović et al. The issues included in this context consist of user traceability, absence of sensor node incognitivity, susceptibility to stolen card assaults, and exposure of the session key.

In their study, Amin et al. [27] identified many vulnerabilities in the system developed by Farash et al. [12]. These weaknesses include compromised anonymity for users, a recognised session-specific spoofing attack, a conventional password-guessing threat facilitated by stolen smart cards, and the presence of unprotected gateway node encryption keys. The researchers used hash functions as a means to develop a patient surveillance system. However, the method used by the previously stated corporation lacks the characteristic of complete secrecy which is forward and is susceptible to remote guessing of password attacks, as demonstrated in reference [13]. Irsad et al. [28] along with Chaudhry et al. (year not specified) have identified the vulnerability of Amin et al.'s (year not specified) methodology to offline guessing of password and impersonation attacks. Das [14] used distinct biometric characteristics including a temporal credential in order to accomplish mutual authentication. In contrast, Wu et al. [15] asserted that Das' method exhibited susceptibility to offline prediction and de-synchronisation attacks. Moreover, Das' methodology was shown to be inadequate in ensuring robust forward security [14].

In the year mentioned, Jiang et al. [16] introduced the Rabin cryptosystem as well as biometric template as a means to establish an effective authenticated key agreement procedure. Nevertheless, the system under consideration is vulnerable to possible threats, like the acquisition of sensor nodes, and fails to provide sufficient assurance for the security of session keys. Furthermore, the used approach provides an additional degree of complexity due to the incorporation of the verification table.

In their study, Amin et al. [17] proposed an approach that leverages the capabilities of IoT-connected gadgets. One of the basic issues faced in the context of IoT ecosystem is the substantial volumes of data produced by many intelligent devices. As a result, computing in the cloud is used to facilitate the manipulation of large quantities of data. However, the used approach is vulnerable to both malicious attacks by insiders and smart card loss attacks.

Jia et al. [18] presented a technique of authentication for an electronic healthcare network operating within a fog server setting throughout the year that was specified. This approach made use of biometric data. The fog nodes are required to perform preprocessing on the data collected from IoT devices and afterwards react to commands from users or the cloud.

Zhang et al. [19] published a paper in 2018 in which they presented a solution for preserving patients' privacy in E-Health systems. This approach makes use of dynamic authentication in conjunction with a three-factor key collaboration process. The assertion was made that the biometric verification might be performed on the server, although the server itself would not have access to the biometric data. In place of the more traditional password table, dynamic authentication is utilised for users to log in. This helps to ensure that users remain anonymous. The strategy that was developed by

Zhang et al. has the goal of reducing the costs of calculation and transmission that are connected with computerised healthcare systems, while at the same time guaranteeing that the necessary precautions are taken to protect patient information. This is achieved via the use of hash functions as well as bio-hash functions. In 2019, significant security flaws were found in the methodology presented by Zhang et al. [19], according to the findings of Aghily et al. [20]. These vulnerabilities included user traceability, which is a desynchronisation threat, an internal attack, and a denial-of-service attack.

Consequently, the authors put forth a novel and efficient programme for IoT E-Health systems, encompassing three essential components: three-factor authentication, control of access, and ownership transfer. The primary objective of this proposal is to rectify the limitations present in Zhang et al.'s scheme while simultaneously establishing a mechanism for controlling access that enables a seamless transfer of authority from a patient's current physician to a new one.

The authors Chatterjee [21] introduced a hash-based authentication technique designed specifically for use in wireless body networks of sensors. Significant security flaws were found in the methodology presented by Zhang et al. [19], according to the findings of Aghily et al. [20].

In an identical year, Lee et al. [22] proposed an anonymised user authorisation system that was intended for use in circumstances involving the Internet of Things. As stated by Lee et al. (year), their suggested system was designed to mitigate a variety of security threats, some of which include stolen mobile devices attacks, user pretending to be someone attacks, replay crimes, stolen verification attacks, privileged-insider acts of violence, sensor node impersonation acts of violence, and session-specific temporary data attacks. All of these threats were taken into consideration when designing the scheme. In addition, the goal of their method was to offer a number of different security characteristics, including user confidentiality, untraceability, authentication across gadgets, session key contract, local recognition of users, consumer-friendly username and password changing, and forward secrecy. All of these elements were intended to be implemented. The study conducted by Ya-Fen et al. [23] included a comprehensive analysis of the approach proposed by Lee et al. The researchers found a number of problems, including failures in sensor node authentication and mobile node permission, as well as a replay attack, a denial-of-service assault, and compromised user untraceability.

In the year 2021, a group of researchers headed by Sahoo et al. [8] proposed an authentication mechanism that employs elliptic curve cryptography (ECC). This approach was developed primarily for use with healthcare systems that were facilitated by the Web and the Internet of Things (IoT). Nevertheless, their methodology fails to ensure the anonymity of users. The aforementioned systems based on public-key cryptography exhibit some security vulnerabilities and need time-intensive procedures [8, 23, 24].

In 2022, a quick authentication strategy for e-health applications was suggested by Zhang et al. [25]. Nevertheless, the computing burden associated with their methodology is disproportionately large in contrast.

Basic terms

The next part provides an overview of the mathematical foundations used inside the system.

Elliptic curve

The syntax of E_{lp} *(a, b)* denotes an elliptic curve E_{lp}, which is characterised by its elliptic form and has been assigned over a limited primitive field Z_p. The equation of a non-singular elliptic curve may be expressed as $b^2 = a^3 + mae + n$, where m, n, and Z_p are constants. It is required that the equation satisfies the condition $4a^3 + 27b^2$ mod $p = 0$. The identity element, denoted as O, is defined as either the point at which nothing happens or the location of the point at infinity. Scalar multiplication may be formally defined as the process of repeatedly adding a scalar to itself. Let G denote a chosen basal point in the elliptic curve Ep, where Ep has an order of n. If the value of G exceeds Ep, then the sum of n occurrences of G, denoted as nG, may be expressed as the sum of G added to itself n times.

Hash function

Consider a hash function denoted as H, which is responsible for mapping input data to a hash value or a hash code of defined size. The features that are seen to be characteristic of determinism and collision resistance are as follows:

1. The function H(a) denotes the use of a hashing function H on the input a, yielding the associated hash value. The function that generates the hash H has the characteristic of determinism, meaning that for every given input a, the output H(a) remains consistent. Additionally, the computation of H(a) is performed in an efficient manner.
2. The hash value, referred to as "hash", is the result of applying the hashing function H to the data being entered a. It is represented as a string with a fixed length of characters as well as a numerical number.
3. A hash function is collision-resistant if it is computationally impossible to discover two separate inputs, a and b, that produce the same hash result (that is, H(a) equals H(b) and a not equal to b). This is because it is impossible to find two inputs that produce the same hash result using the same hash function.

Fuzzy extractor

The term "fuzzy" is associated with the predefined values used in the use of cryptography which are derived from values that have a resemblance to, but not an exact replication of, the original key, thereby ensuring the requisite degree of security remains intact. Fuzzy extractors employ a combination of functions to generate secure keys, handle variations or errors, and enable reliable authentication in the presence of slight differences in the input data. Yevgeniy et al. [29] proposed the use of an extractor to remove a nearly randomised string "s" from the biometrical input 'i_p' with a degree of tolerance for errors. When there is a change in the input, but it stays in proximity to the initial input, a fuzzy extractor is capable of extracting the same output. In order to get the IP address from a fresh biometrical input, a uniformly randomised string is constructed by the use of the following two operations:

1. The generation function (Gen) can be expressed formally as Gen(i_p) = (s,r), where i_p' represents the input. The programme produces an outcome of a randomly generated string, denoted as s, within the range of {0, 1}, together with an auxiliary string, denoted as *r*.
2. The Reproduction function (Rep) is designed to accept a noisy biometric input (i_p) and its matching random auxiliary string (r) in order to recover the original string (s). The function may be represented as Rep(i_p',r) = s.

Security requirements

Ensuring robust protection of patients' privacy is of paramount importance within e-health systems. Based on the actual circumstances, an authentication method for the system mentioned above must satisfy the following criteria.

1. The occurrence of resistance in response to many recognised attacks. The authentication system should demonstrate the capacity to successfully counteract several prevalent e-health attacks, including impersonation attacks, as well as other similar threats.
2. Mutual authentication is the procedural mechanism whereby both parties engaged in a communication transaction mutually validate and confirm each other's identities. Once the implementation of the system for authentication has been completed, it becomes essential for both the individual receiving treatment and the healthcare server to undergo authentication procedures in order to ensure effective communication.
3. The concepts of anonymity and untraceability. The preservation of patient privacy has the utmost importance within the healthcare industry. The proposed methodology should ensure the concealment and non-traceability of patients' authentic identities inside the text messages they transmit.
4. Biometric protection refers to the use of biological characteristics, such as fingerprints, iris patterns, or facial recognition, as a means of safeguarding access to sensitive information or physical. Patients should not have to be apprehensive about the potential disclosure of their biometric data when employing e-health services. Consequently, in the context of patient identification by biometric data, it is essential for the system to provide robust safeguards for biometric information.
5. The notion of three-factor anonymity is a basic concept within the realm of information security. Maintaining the secrecy of a patient's personal information is of utmost importance, even in the scenario when two keys are revealed to an unauthorised entity. In order to safeguard patient confidentiality, it is essential that the system include a three-factor secrecy mechanism.

Threat model

According to e-health system security criteria, an adversary A against the proposed method is an active attacker who is assumed to have access to the message passing through the network and has the capabilities provided in the following:

1. A owns authority over the communication channel and possesses various attacks throughout the execution phase, such as intercepting messages, postponement, replaying, deletion, and modification.
2. A sort of channel attack is executed by A in order to get the confidential information retained on the user's smart card.
3. Power analysis and reverse engineering methodologies may be used to extract confidential data from smart cards.
4. A potential attacker has the capability to compromise either the secret key, smart card information, password, and biometric information individually, but not all of these elements simultaneously.
5. An individual may be categorised as either a member of the insider group or an outsider.

Problem formulation

According to the research that has been done, it is found that many smart card-based as well as biometric-based authentication techniques are suggested for use in health care systems that use RSA, ECC, and other encryption algorithms. On the other hand, the majority of these plans have not been able to protect against all of the known security risks. In this scenario, an authentication strategy that makes use of ECC and is enabled by the IoT has been developed. This approach defeats the majority of the recognised security risks.

Proposed system

In this discourse, it delves into the intricacies of the anonymous three-way authentication technique specifically designed for Internet of Things (IoT) healthcare applications. Table 1 presents a comprehensive overview of the symbols and abbreviations used throughout the course of this scholarly article.

The proposed system consists of three key participants: the Telecare server (Tj), a patient (Pi), and a registered centre (R). The composition consists of five stages as shown in Fig. 1, which will now be examined, and Fig. 2 represents the flowchart of the model.

Initialisation phase

The enrollment centre (R) chooses a non-singular elliptical curve $E_{\mathrm{lp}}(x,y)$ spanning a finite field Z_{p} in order to initialise the entire system.

A large prime number p is selected from the finite field Z_{p} associated with an elliptic curve. The variable R chooses a point Pt from the curve $E_{\mathrm{lp}}(x,y)$ inside the finite field Z_{p}. The user proceeds by selecting a master key, denoted as mk, and then calculates the public key, Pub, as the product of mk and Pt. Subsequently, R generates a pair (a, b) and designates the private key as (a, b, mk), whereas (E_{lp}, Pt, Pub) is designated as its public key.

Registration phase

This stage encompasses two distinct stages: the server enrollment phase as well as the patient enrollment step. The steps for enrollment are outlined in Table 2.

Table 1 Notation summary

Notation	Description
P_i	i^{th} Patient/user
T_j	j^{th} Telecare medical server
$\mathrm{SI_j}$	Server (j^{th}) identity
PID_i	Patient (i^{th}) identity
PP_i	Patient (i^{th}) password
mk	Shared private key among R and T_j
K_{SP}	Session key (Server and Patient)
II	Concatenation operation
A_s	Auxiliary string
R	Registration centre
S	Smart card
RI	Registration Centre Identity
PB_i	Patient ($\mathrm{i^{th}}$) Biometric
$h(x\|y)$	Master key by R
$\oplus$	Ex-OR operation
$h()$	One-way secure hash function
{}	Message exchanged
RN	Random number
$\mathrm{Gen(w)} = (R_s, A_s)$	i/p(w) R_s —Random string A_s—Auxiliary string
A_{dvk}	Adversary
$E(k)$	Encryption
$D(k)$	Decryption

Telecare server enrollment

The telecare server, denoted as T_j, begins the registration process by executing a series of procedures to establish its connection with the registration centre.

Step 1: The server autonomously determines its identification SI_j and it transmits to the enrollment centre via a safe communication channel.

Step 2: When a message is received, the R initiates a process wherein it creates a random number, denoted as $\mathrm{RN_j}$. Subsequently, the R proceeds to calculate $\mathrm{RN_{1j}}$, which is derived from the concatenation of RN_j with the hash of the concatenation of x and y as $RN_{1j} = h(RN_j||h(a||b))$. Here, x and y represent the master keys that have been created by the signing-up centre. Subsequently, the software programming language R saves the variables $\mathrm{RN_{1j}}$ and $\mathrm{SI_j}$ and proceeds to transmit the variable $\mathrm{RN_{1j}}$ exclusively to the entity $\mathrm{T_j}$ over a secure communication channel, with the intention of preserving it for further use.

Phase of patient registration

The registration process for a new patient at the registration centre involves the following phases.

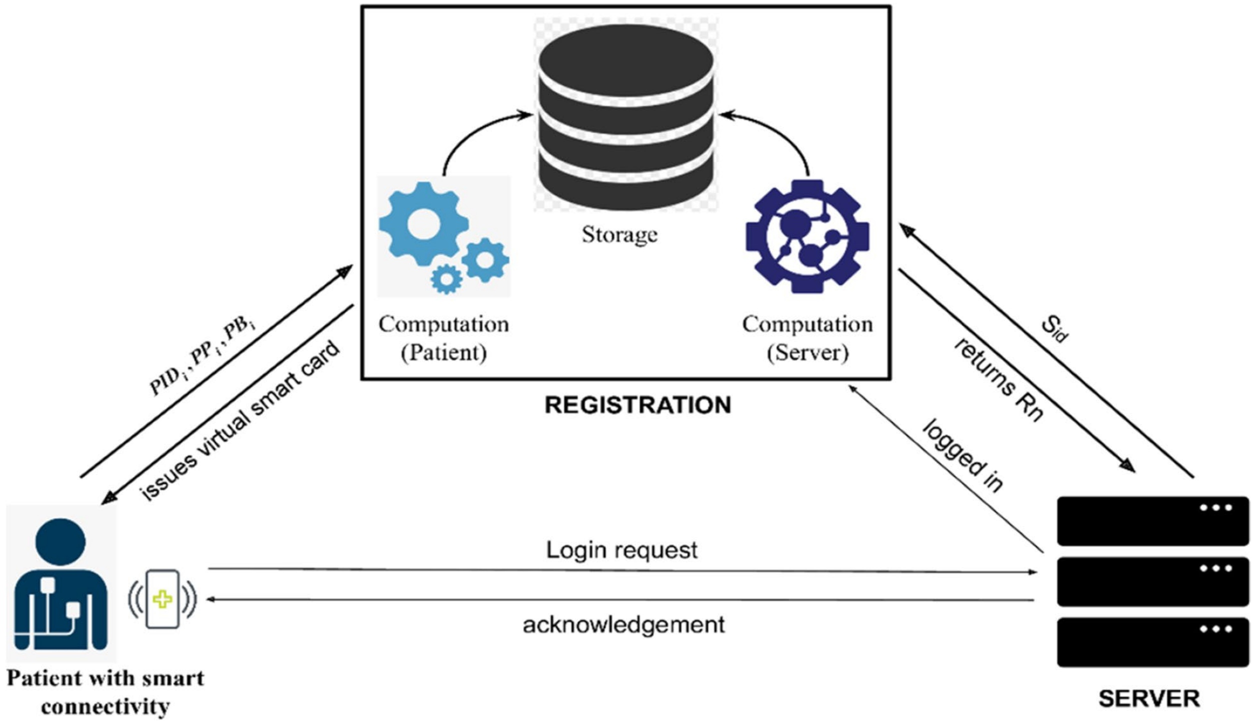

Fig. 1 System architecture

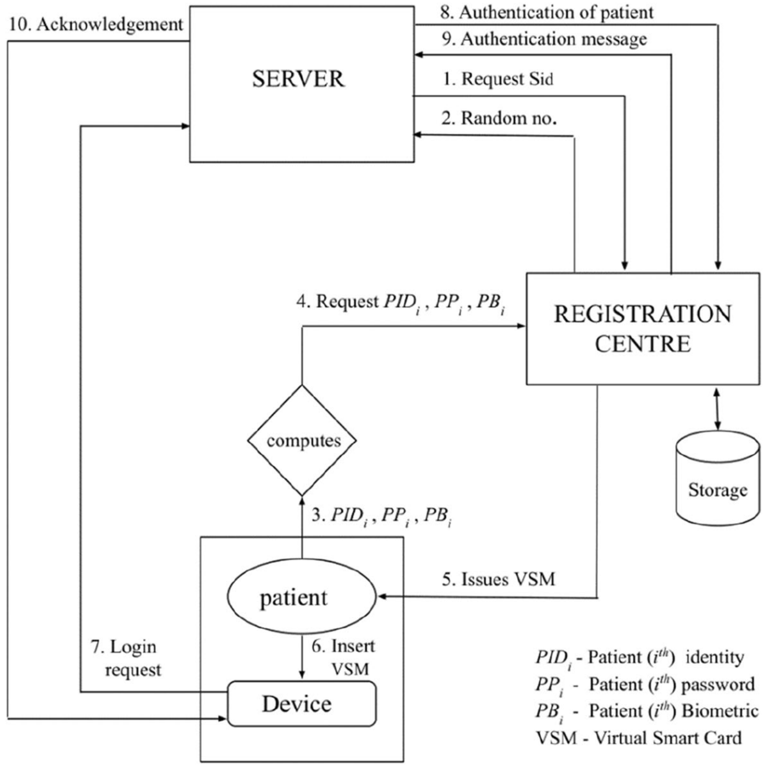
10. Acknowledgement
SERVER
8. Authentication of patient
9. Authentication message
1. Request Sid
2. Random no.
4. Request PID_i , PP_i , PB_i
REGISTRATION CENTRE
computes
Storage
3. PID_i , PP_i , PB_i
5. Issues VSM
patient
7. Login request
6. Insert VSM
Device
PID_i - Patient (i^{th}) identity
PP_i - Patient (i^{th}) password
PB_i - Patient (i^{th}) Biometric
VSM - Virtual Smart Card

Fig. 2 Flowchart of proposed work

Table 2 Registration phase

Server registration phase		
Telecare Medical Server (Tj)		Registration centre (R)

Selects SI,	– {SI}
	← {RN_{1i}}
		Generates a random number
		RN1j = h(RN_j||h(a||b))
		Stores {RN_{1j}, SI_j}

Stores {RN_1}}		
Patient registration phase		
Patient/User P		Registration centre (R)

Selects a sensor SN
Choose PID, PW biometric PB,
Compute Gen(PB)=(σ_i, θ_i)
	→ {PID, PP_i, PB_i, SN_i} ← {B_i, C_1, G_i, h(.), E_k, D_k}	B = h(PID||PP||PP;)
		C = SN ⊕ h(a||b) ⊕ h(R1||x)
		G_i = h(RI|x) ⊕ h PID||PP_{i1})
		Stores {PIDi, A_j, C_i}

	Secure Channel → Insecure Channel →	

Step 1: The individual, denoted as P_i, exercises autonomy in selecting their Personal Identification Number (PID_i), and password (PP_i), and then provides their biometric data (PB_i) to the sensor.

Step 2: Next, P_i employs the fuzzy extractor to calculate Gen(BM_i) = (σ_i, θ_i). The individual performs a computation to generate their password, denoted as $PP_{i1} = h(PP_i||\sigma_i)$, and then sends a registration request message, represented as {PID_i, PP_{i1}, PB_i, SN_i} to the entity referred to as R.

Step 3: The computation of A_i in the R programming language involves the use of the function h, which takes as input the concatenation of $\mathrm{PP}_{1\mathrm{i}}$ and PB_i as $A_i=h(PP_{1i}||PB_i)$. $P=(P_x,P_y)$. Let $P=(P_x,P_y)$ be the coordinates of a point. B_i is calculated as $B_i=h(PID_i||PP_i||PB_i)$, where PID_i, PP_i, and PB_i are specific values. C_i is computed as $C_i=SN_i \oplus h(a||b) \oplus h(R1||x)$, where SN_i, x, y, and R_1 are specific values. Similarly, G_i is determined as $G_i=h(RI||x) \oplus h(PID_i||PP_{i1})$. In conclusion, the system saves the variables $\{\mathrm{PID}_\mathrm{i}, \mathrm{A}_\mathrm{i}, \mathrm{C}_\mathrm{i}\}$ in the R storage for future reference and provides the patient with the output S, accompanied by the parameters as follows $\{B_i, C_i, G_i, h(.), E_k, D_k\}$.
Step 4: Once the S has been acquired, the patient proceeds to put the parameters θ_i to the chip on the smart card. The set S is comprised of the following parameters: B_i, C_i, G_i, $h(.)$, E_k, D_k, and θ_i.

Login phase

To access the remote healthcare server T_j, the individual receiving care must do the steps as follows:

Step 1: The individual proceeds to put their electronic card into the designated card reader and proceeds to imprint their biometric PB_i onto the corresponding device. Additionally, the user provides their username (PB_i) in conjunction with their password (PP_i). Next, we calculate as $\sigma_i^* =Rep(PB_i,\theta_i)$. Then, we compute $PP_{i1}^* =h(\mathrm{PP}_\mathrm{i}||\sigma_i^*)$, $B_i^* \overset{?}{=} h(PID_i||PP_{i1}^*||PB_i)$.
Step 2: Next, a comparison is made between the calculated value of B_i^* and the one obtained parameter B_i. In the event that the requirement is not met, S concludes the login phase.

Alternatively, it proceeds to the subsequent stage.

Step 3: The smart card starts the generation of a random integer, denoted as n_1, and proceeds to compute $A_i^* = h(PP_{i1}^*||PB_i).P(P_x, P_y)$. The probability of event P_x and P_y occurring simultaneously is denoted as $P(P_x, P_y)$. Let M_1 represent the product of n_1 and P, whereas M_2 represents the product of n_1.The equation may be expressed as follows in an academic manner: $M_1=n_1.P$, $M_2=n_1.Pub$, $M_3=n_1 \oplus h(PID_i ||C_i||A_i^* ||T_u)$, $M_4=h(PID_i ||M_1||A_i^*||n_1||T_u)$, $M_5=E_{(SNi||h(RI||x)} (ID_i||M_3||P_y)$. The acquisition of a registration ID is restricted to those who possess the necessary authorisation. Subsequently, the notification $\{M_4, M_5, C_i, P_y\}$ is forwarded to the authorisation centre via the common accessed channel.

Authentication phase

Upon receiving the request to login from entities M_4, M_5, C_i, and T_u, both entity R and server T_j proceed to carry out a series of actions in order to successfully establish mutual authentication among the server and the user requesting the service.

Step 1: The first step is the verification of the login information by calculating T_r, which must be less than or equal to the value of threshold ΔT. If the condition is satisfied, R performs the computations $SN_i^*=h(a||b) \oplus C_i \oplus h(RI||x)$, $D_{(SNi||h(RI||x}$

> $_{))}(M_5)=(ID_i||M_3||P_y)$, $n_i^*= M_3 \oplus h(PID_i\ ||C_i||A_i||T_u)$, $M_1^*= n_i^*.P$, $M_2^*=n_i^*.Pub$ and compares $M_4^* \overset{?}{=} h(PID_i||M_1^*||A_i||n_1^*)$. If the condition is satisfied, then R computes $M_6=h(PID_i||SI_j||M_1^*||\ R_{1j}||T_r^*)$, $M_7=E_{(R1j)}\ (PID_i||M_1^*||P_y)$ and sends {M_6, M_7, T_r^*} to the T_j through insecure channel.
>
> Step 2: After receiving the authentication information message, T_j validates the time stamp by checking whether $T_{\mathrm{s}} - T_{\mathrm{r}}^*$ less than or equal to $\Delta\mathrm{T}$. Whether the condition is met, T_j proceeds to decrypt $D_{(R1j)}\ (M_7)=(\mathrm{PID}_i||M_1^*||P_y)$ and checks $M_6 \overset{?}{=} h(\mathrm{PID}_i||\mathrm{SI}_j||M_1^*||R_{1j}||T_{\mathrm{r}}^*)$. If the specified condition evaluates to true, a random number, denoted as n_2, is generated and then used to determine the value of S_1, which is assigned the value of n_2. In the given expression, Pub, S_2 represents the concatenation of the variables $\mathrm{PID_i}$, $\mathrm{SI_j}$, and $\mathrm{P_y}$, which are hashed using the function h(). SK is equal to $\mathrm{n_2}$. $\mathrm{M_2}^*$ denotes an unspecified value. S_3 is obtained by concatenating $\mathrm{PID_i}$, $\mathrm{SI_j}$, S_1, and $T_S{}^*$ and then hashing the result using the function $h()$. S_4 is the result of encrypting the concatenation of $\mathrm{PID_i}$, P_y, S_1, and $\mathrm{S_2}$ using the Subsequently, $\mathrm{T_j}$ transmits the set {$\mathrm{S_3}$, $\mathrm{S_4}$, $\mathrm{T_s}^*$} to $\mathrm{P_i}$ over an unsecured communication channel.
>
> Step 3: Upon receipt of the communication from T_j, P_i proceeds to validate the time stamp by ensuring that the difference between the updated time $T_u{}^*$ and the original time $T_s{}^*$ is less than or equal to the specified time interval ΔT. If the condition is true, the value of $D_h(PID||P_y)(S_4)=(S_1||S_2)$. Additionally, SK* is determined as $SK^*=n_1.S_1$, $S_3^* \overset{?}{=} h(PID_i||SI_j||S_1||SK^*||T_s^*)$. Finally, the value of $M_8=h(PID_i||S_2||SK^*||T_u^*)$ and sends {M_8, T_u^*} to the server for verification. P_i then transmits the values {M_8, $T_{\mathrm{u}}{}^*$} onto the server's memory for the purpose of verification.
>
> Step 4: The T_j entity gets the inputs M_8 and $T_u{}^*$ and proceeds to verify the condition $T_s^{**} - T_u^{**} \leq \Delta T$. If the verification is satisfied, then it checks the equation $M_8^* \overset{?}{=} h(PID_i||S_2||SK^*||T_u^*)$. Once the verification process is completed, successful session key agreements and mutual authentication have been achieved between the patient's device and the server providing telecare service. Consequently, both parties are now prepared for communication. Table 3 provides a concise overview of the login and authorisation stages.

Password reset

During this particular stage, a valid patient (referred to as P_i) has the ability to modify their password by completing the subsequent procedures.

> Step 1: The individual known as P_i proceeds to place their identification card onto a card reader, then enter their unique personal identification number ($\mathrm{PID_i}$) and password ($\mathrm{PP_i}$) and imprint their biometric data (PBi). Next, the computation of $\sigma_i^*=Rep(PB_i,\theta_i)$, $PP_{i1}^* = h(\mathrm{PP_i}||\sigma_i^*)$. Now, S verifies $B_i^* \overset{?}{=} h(PID_i||PP_{i1}^*||PB_i)$. In the event that the requirement is not met, the smart card will reject the request for a password update and terminate the connection. Alternatively, the patient is requested to input a new password denoted as PP_i^{new}.
>
> Step 2: The symbol S is responsible for calculating the new value of $PP_{i1}^{new}=\mathrm{h}(PP_i^{new}||\sigma_i)$. Finally, S replaces B_i with B_i^{new}. Similarly, the value of $B_i^{new}=h(PID_i||PP_{i1}^{new}||(PB_i))$ is determined using the function h with inputs Ultimately, the element S substitutes the element B_i with a new element denoted as B_i^{new}.

Table 3 User authentication phase

Patient (Pi)	*Registration centre (R)*	*Telecare server (T_j)*
Inputs PID, PP, PB, *S Computes* $a; = Rep(PB,0;)$ $M_1 = n_1.P, M_2 = n_1.Pub, M_3 = n_1 \oplus h(PID_i \Vert C_i \Vert A_i^* \Vert T_u), M_4 = h(PID_i \Vert M_1 \Vert A_i^* \Vert n_1 \Vert T_u),$ $M_5 = E_{(SNi \Vert h(RI \Vert x)} (ID_i \Vert M_3 \Vert P_y)$ $(M_4, M_5, C_i, T_u) \rightarrow$		
	Verify $T_r < = \Delta T$*. If True* $SN_i^* = h(a \Vert b) \oplus C_i \oplus h(RI \Vert x),$ $D_{(SNi \Vert h(RI \Vert x))} (M_5) = (ID_i \Vert M_3 \Vert P_y), n_i^* = M_3 \oplus h(PID_i \Vert C_i \Vert A_i \Vert T_u),$ $M_1^* = n_i^*.P, M_2^* = n_i^*.Pub\ M_4^* \overset{?}{=} h(PID_i \Vert M_1^* \Vert A_i \Vert n_1^*)$ *If true,* $M_6 = h(PID_i \Vert SI_j \Vert M_1^* \Vert R_{1j} \Vert T_r^*), M_7 = E_{(R1j)} (PID_i \Vert M_1^* \Vert P_y)$ $\{M_6, M_7, T_r^*\} \rightarrow$ *insecure channel*	
		$T_s — T_r^* \leq \Delta T$ *If satisfied* $D_{(R1j)} (M_7) = (PID_i \Vert M_1^* \Vert P_y)\ M_6 \overset{?}{=} h(PID_i \Vert SI_j \Vert M_1^* \Vert R_{1j} \Vert T_r^*)$*. If true, then generates a random number* n_2 $S_1 = n_2.Pub, S_2 = h(PID_i \Vert SI_j \Vert P_y), SK = n_2. M_2^*,$ $S_3 = h(PID_i \Vert SI_j \vert S_1 \vert \Vert T_S^*), S_4 = E_{h(PIDi \Vert Py)}(S_1 \Vert S_2)$
	$\leftarrow \{S3, S4, T_s^*\}$	
$T_u^* - T_s^* \leq \Delta T$*. If satisfied* $D_h(PID \Vert P_y) (S_4) = (S_1 \Vert S_2),$ $SK^* = n_1.S_1, S_3^* \overset{?}{=} h(PID_i \Vert SI_j \Vert S_1 \Vert SK^* \Vert T_s^*)$*. If* $S_3^* = S_3,$ $M_8 = h(PID_i \Vert S_2 \Vert SK^* \Vert T_u^*)$ $\{M_8, T_u^*\} \rightarrow$		
		$T_s^{**} - T_u^{**} \leq \Delta T$*. If true, then check* $M_8^* \overset{?}{=} h(PID_i \Vert S_2 \Vert SK^* \Vert T_u^*)$ *Verified key for the session*

Analysis of security measures

This section encompasses an examination of formal as well as informal security analysis methodologies. The BAN logic framework was used to illustrate the process of mutual authentication inside our system. Subsequently, we engaged in a discourse pertaining to the informal security analysis of the suggested system.

A formal analysis of security measures

The BAN logic is employed to rigorously evaluate the accuracy of the two-way authentication method implemented in our model. To apply BAN logic to the TMIS ECC authentication scheme described, defined initial beliefs, messages exchanged, and the BAN logic inference rules to the Telecare server registration phase are as follows:

Beliefs:

- Initially, the registration centre (R) believes {RN_j, SI_j} (Step 2)
- Initially, the telecare server (T_j) believes its own identity SI_j (Step 1)

Messages exchanged:

- T_j sends SI_j to R (Step 1)
- R sends RN_j to S_j (Step 2)

BAN logic inference rules:

> Belief rule 1: If a principal P_1 believes a statement X, and P_1 receives a message M containing X, then P_1 believes that the sender of M believes X.

Applying the BAN logic inference rules:

1. From Step 1: T_j believes SI_j.
2. From Step 2: R generates $\mathrm{RN_j = h(R \| h(x \| y))}$ and sends $\{\mathrm{RN_j}\}$ to $\mathrm{T_j}$.
   - $\mathrm{T_j}$ receives $\{\mathrm{RN_j}\}$ and believes that R believes $\{\mathrm{RN_j}\}$.
3. From Step 2: R stores $\{\mathrm{RN}_j, \mathrm{SI}_j\}$.
   - R believes $\{\mathrm{RN}_j, \mathrm{SI}_j\}$.

By applying the belief rule, we can infer that T_j believes R believes $\{\mathrm{RN_j}, \mathrm{SI_j}\}$.

This paper presents a comprehensive examination and elucidation of the individual stages involved in the Telecare server registrations phase, taking into account the distinct security prerequisites as well as assumptions of the architecture for TMIS ECC authentication technique using BAN logic:

> *Step 1:* The server autonomously determines its unique identifier, denoted as $\mathrm{SI_j}$, and transmits it to the enrollment centre through a secure communication channel.
>
> *Explanation:* The Telecare server, denoted as T_j, selects its unique identification $\mathrm{SI_j}$ and securely transmits this information to the registration centre, denoted as R. This stage is responsible for establishing the identity of the server.
>
> *Step 2:* When a message is received, the R entity proceeds to produce a random number denoted as $\mathrm{RN_j}$. Subsequently, it computes the value of $\mathrm{RN_j}$ using the formula $\mathrm{RN}_j = h(R \| h(x \| y))$, wherein x and y represent the master keys provided by the registration centre. Subsequently, the data $\{\mathrm{RN}_j, \mathrm{SI}_j\}$ is stored in R and sent $\{\mathrm{RN}_j\}$ to S_j through a secure communication channel for further use.
>
> *Explanation:* The receiving component (RC) is in receipt of the message that includes the identification (SI_j) of the server. The algorithm produces a pseudo-random number RN_j by concatenating the value of R along with the hash that represents the concatenation of variables x and y. The R stores the pair $\{\mathrm{RN}_j, \mathrm{SI}_j\}$ for future reference and sends the random number RN_j to T_j through a secure channel. This step establishes a shared random value between RC and T_j for further communication.

BAN logic inference:

1. T_j believes SI_j.

Explanation: Since T_j selected $\mathrm{SI_j}$ and sent it to R, T_j believes in its own chosen identity.

2. T_j receives $\{\mathrm{RN_j}\}$ from R and believes that R believes $\{\mathrm{RN}_j\}$.
   Explanation: T_j receives the random number RN_j from R, indicating that R believes in the existence of RN_j and its association with the server. Therefore, T_j believes that R believes in the pair $\{\mathrm{RN}_j\}$.
3. R stores $\{\mathrm{RN}_j, \mathrm{SI}_j\}$ and believes $\{\mathrm{RN}_j, \mathrm{SI}_j\}$.
   Explanation: R receives and stores the pair $\{\mathrm{RN}_j, \mathrm{SI}_j\}$, indicating that R believes in the existence of both RN_j and SI_j and their association with the server. Therefore, R believes in the pair $\{\mathrm{RN}_j, \mathrm{SI}_j\}$.

Based on the analysis conducted, it can be deduced that T_j has the belief that R also holds the belief in $\{\mathrm{RN}_j, \mathrm{SI}_j\}$. The aforementioned study demonstrates that the suggested approach is capable of achieving mutual authentication.

Analysis of informal security measures

The proposed model incorporates several security measures that can defend against various types of attacks. Here are some potential attacks that the model can defend against:

1. *Unauthorised access:* The model includes a patient (P_i) who registers with the centre (R) and receives authentication parameters. This helps prevent unauthorised users from accessing the system.
2. *Impersonation attacks:* The use of biometric data ($\mathrm{PB_i}$) and password-based authentication ($\mathrm{PP_i}$) helps to authenticate the patient during the login phase. This defends against impersonation attacks where an attacker tries to pretend to be a legitimate user.
3. *Replay attacks:* The registration and login phases involve the use of random numbers (RN_{1j}, n_1, n_2) and timestamp verification. These measures protect against replay attacks, where an attacker tries to intercept and gain unauthorised access.
4. *Man-in-the-middle attacks:* The proposed model uses secure channels for communication, such as a secure channel between the server ($\mathrm{T_j}$) and the registration centre (R). This helps protect against interception and modification of messages by attackers attempting to impersonate one of the parties involved.
5. *Password guessing attacks:* The system employs password hashing (h) and combines it with a patient-specific value (σ_i) during the registration phase and also allows legitimate users to change their passwords. This makes it computationally difficult for an attacker to guess the patient's password ($\mathrm{PP_i}$) based on the stored hash value.
6. *Biometric spoofing attacks:* The system incorporates biometric authentication using the patient's biometric data (PBi). By imprinting the biometric data at the sensor during registration and login phases, the system can defend against spoofing attacks that attempt to bypass biometric authentication.

Hence, our model is resistant and provides security against all these types of attacks.

Security requirement discussion

User anonymity

The user's true identity is only revealed during the registration and authentication phases. However, during the authentication process, the user only inputs his or her identification while logging in. Throughout the authentication procedure, HIDi safeguards the user's identity. As a result, our protocol ensures anonymity and untraceabilty.

Biometrics protection

The proposed approach secures biometric information during the authentication procedure. The use of hash functions and secure symmetric encryption algorithms ensures the safeguarding of patients' biometric information that is encoded inside sent messages.

3-Factor secrecy

The concept of secrecy encompasses three fundamental elements, namely a security code, a smart card, and biometric data. Based on prior research, the essential factors for initiating an attack to calculate the key to the session are denoted as A1 and Pi. Permit A to decide on any two out of the three criteria.

(1) Both a password along with a smart card have to be used for authentication. Even in the event that individual A has knowledge of the password and possesses the capability to extract the required parameters from SC, they are unable to ascertain the values of A_1 and P_i for any kind of attack.

(2) The topic of discussion pertains to the use of biometrics and passwords in the context of authentication and security measures. In order for individual A to calculate A_1, it is necessary for them to possess both the password along with biometric data, as well as have knowledge of A_2 and P_i. However, A_2 is stored on a smart card.

(3) The computation of $A_1 = A_2 \oplus P_i$ is not feasible without prior knowledge of the relevant information on PW_i and ID_i, even after the acquisition of the biometric as well as smart card.

As a result, our technique provides three-factor confidentiality.

Performance evaluation

In this part, a comparative analysis is conducted to assess the communication cost and computing cost of our work in relation to earlier related methodologies [8, 17, 24, 25].

According to the findings presented in Table 4, this system has been demonstrated to possess a high level of security, effectively countering many well-documented assaults. Furthermore, it fulfils a greater number of security criteria compared to other comparable schemes mentioned in Fig. 3, as evidenced by previous studies [8, 17, 24, 25].

The proposed methodology prioritises the safeguarding of user privacy via the incorporation of electronic card as well as biometric authentication elements, as well as the provision of user anonymity. These features are essential for the successful deployment of e-health systems within the context of SIoT. The protection of user personal information is of utmost importance, making it imperative to provide both user untraceability

Table 4 Security features comparison with comparable scheme

Features concerning security	Amin et al.	Yang et al.	Zhou et al.	Sahoo et al.	Proposed three-factor scheme
Replay attacks	Satisfies	Satisfies	Satisfies	Satisfies	Satisfies
DoS attacks	Satisfies	No	Satisfies	Satisfies	Satisfies
Man-in-middle attack	Satisfies	Satisfies	Satisfies	Satisfies	Satisfies
Impersonation attacks	Satisfies	Satisfies	Satisfies	Satisfies	Satisfies
User anonymity	No	No	Satisfies	Satisfies	Satisfies
Perfect forward secrecy	Satisfies	Satisfies	No	Satisfies	Satisfies
Secure password update	Satisfies	No	Satisfies	Satisfies	Satisfies
Biometrics protection	-	-	-	Satisfies	Satisfies
Untraceability	No	No	No	No	Satisfies
Mutual authentication	Satisfies	Satisfies	Satisfies	Satisfies	Satisfies
Password guessing attacks	No	Satisfies	Satisfies	Satisfies	Satisfies

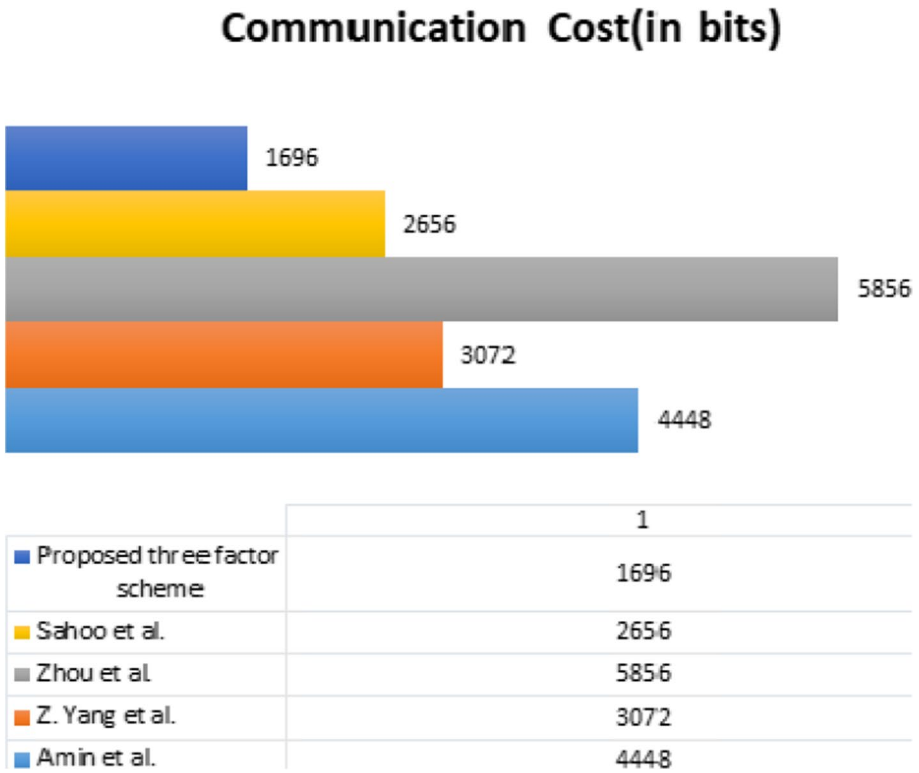

Fig. 3 Communication cost (bits) comparison with comparable scheme

and anonymity. Nevertheless, the technique proposed by Amin [17] and the scheme proposed by Yang et al. [24] do not fulfil the criteria of user anonymity and untraceability. The approach proposed by Amin et al. [17] lacks the property of full forward secrecy and is vulnerable to password-guessing attacks. The technique proposed by Zhou [25] does not effectively provide comprehensive forward confidentiality and untraceability. The approach proposed by Sahoo [8] does not guarantee user untraceability. Based on the findings shown in Table 4, our proposed technique demonstrates superior security

Table 5 Computational cost comparison with state-of-the-art approaches

Scheme	User	Registration centre (R)	Trusted server (T)	Total cost
Jia et al.	$5_{\mathrm{TH}}+2_{\mathrm{TL}}+1_{\mathrm{TB}}$	4TH + 2TL + 1TB	9TH + 3TL + 1TB	18TH + 7TL + 3TB ≈1113ms
Amin et al.	9TH	10TH	4TH	23TH ≈ 1.1ms
Yang et al.	20TH	19TH	17TH	37TH ≈ 1.34ms
Sahoo et al.	8TH + 3TL + 2TN	3TH + 2TL + 2TN	4TH + 2TL + 2TN	15TH + 7TL + 6TN ≈ 178.1ms
Proposed scheme	5TH + 1TbH + 2TN	2TH + 1TbH + 2TN	4TH + 1TbH + 6TN	11TH + 3TbH + 10TN ≈ 0.372ms

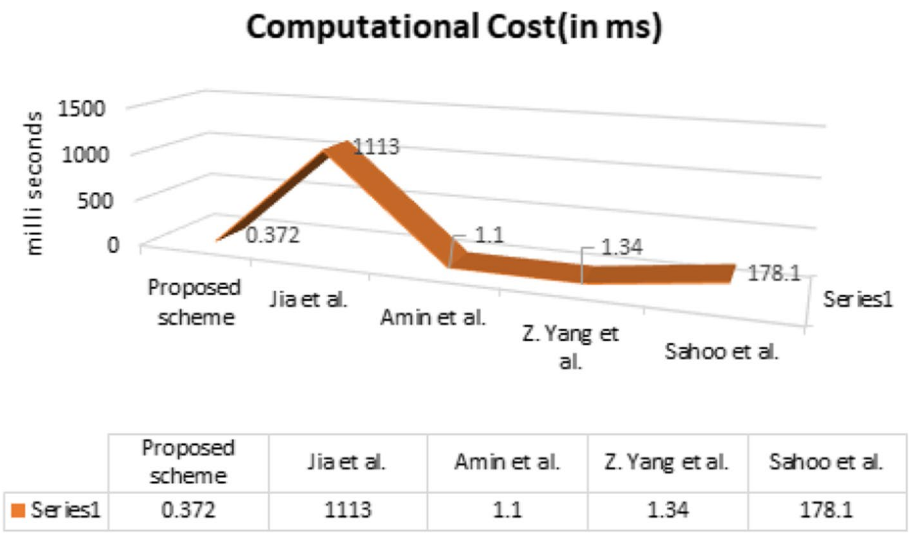

Fig. 4 Comparison of computational cost

characteristics and enhanced resistance against several established threats compared to the methodologies proposed by Amin et al. [17], Yang et al. [24], Zhou et al. [25], and Sahoo et al. [8].

Subsequently, we proceed to evaluate the computational expenditure of our proposed methodology in contrast to existing methods [8, 17, 18, 24], as seen in Table 5. The following explanations provide several meanings of notations:

T_{N}: The duration necessary for the execution of the symmetric key encryption/decryption process.
T_{H}: Function for Hashing
T_{L}: Multiplication of elliptic points as an operation
T_{B}: Bilinear pairing
T_{bH}: Biometric hashing function

Based on the data presented in Fig. 4 and Table 5, it can be observed that Amin's scheme has an overall execution time of 1.1 ms, Yang's approach requires an overall execution period of 1.34 ms, Jia's scheme has an overall execution time of 1113 ms, Sahoo's approach exhibits an execution time of 178.1 ms, and the proposed approach demonstrates an execution time of 0.372 ms. Despite the somewhat increased computing cost, the proposed approach exhibits considerably enhanced security compared to currently available similar techniques.

In our study, it is assumed that the function of hashing identity/password/ECC, and encryption/decryption have lengths of 160 bits, 160 bits, and 128 bits, respectively. This assumption is made for the purpose of analysing communicational costs. In addition, it is worth noting that the randomly generated number/time stamp has a length of 32 bits. Throughout the login phase with one another, the user transmits a message consisting of M_4, M_5, C_i, and T_u to the registration centre. This message needs a total of 608 bits, calculated by summing the bit lengths of each component (160 bits for M_4, 256 bits for M_5, 160 bits for C_i, and 32 bits for T_u). During the authentication stage, messages such as $\{M_6, M_7, T_\mathrm{r}\}$, $\{S_3, S_4, T_\mathrm{s}\}$, $\{\mathrm{M}_8, T_\mathrm{u}^{**}\}$ need a total of 448 bits, 448 bits, and 192 bits, respectively. The cumulative cost of these messages amounts to 1696 bits. Our proposed method exhibits a reduced communication of up to 71.03% cost in comparison to other schemes already in existence.

The suggested methodology incorporates fundamental security safeguards and demonstrates resilience against a range of well-documented attack vectors. The scheme's cost-effectiveness in terms of computation and communication expenses suggests its viability for practical implementation in many real-world applications. The implementation of BAN logic has been shown to effectively achieve safe authentication between parties and session key consensus. The formal and informal analyses of our system demonstrate its resilience against typical security threats.

Conclusions

By placing a high emphasis on security measures, healthcare organisations may effectively safeguard patient data and guarantee the secure and dependable functioning of the Telemedicine Information System (TMIS) connected with the Internet of Things (IoT) in wellness settings. Three-factor dependent mutual authentication techniques are considered to be the optimal option for e-healthcare applications within the context of Social Internet of Things (IoT). The proposed methodology in this research entails the use of an authentication system, including password, smart card, and biometric authentication. This approach is shown to be notably more effective and robust in terms of efficiency and security. The system employs a comprehensive methodology that integrates both ECC and Hash techniques, hence guaranteeing the confidentiality and integrity of patient data. By using this authentication system, the preservation of the user's anonymity is ensured, and the user is granted the ability to modify their password as required. The suggested approach underwent a comprehensive evaluation, including both BAN logic along with informal security analysis. The results of this evaluation indicate that the technique exhibits a high level of resistance against a wide range of authentication assaults. In addition, our methodology demonstrates lower computational cost along with communication costs (of up to 71.03%) as compared to existing validated approaches in the same domain. A potential weakness and limitation of our model could be its vulnerability to device compromise and to address this limitation, the model can be enhanced by integrating Hardware Security Modules (HSMs) into IoT devices to securely store cryptographic keys and perform critical security operations. Future research involves the development of an Intrusion Detection along with Monitoring system as well as an Identity Access Management system to regulate access to both the TMIS and SIoT platforms.

Acknowledgements
The authors thank the Editor and reviewers for their insightful comments to improve the manuscript.

Authors' contributions
Arpitha T* (corresponding author): conception and design of the study, implementation, acquisition of data, analysis, and/or interpretation of data, writing—original draft. Dharamendra Chouhan: guidance, reviewing, and editing the paper. Shreyas J: reviewing and editing the paper. All authors have read and approved the manuscript.

Funding
No funding is available for this research.

Availability of data and materials
Data sharing does not apply to this article as no datasets were generated or analysed during the current study.

Declarations

Competing interests
The authors declare that they have no competing interests.

Received: 25 September 2023 Accepted: 8 December 2023
Published online: 03 January 2024

References

1. Karuppiah M (2016) Remote user authentication scheme using smart card: a review. Int J Internet Protoc Technol 9(2/3):107–120
2. Karuppiah M, Kumari S, Das AK, Li X, Wu F, Basu S (2016) A secure lightweight authentication scheme with user anonymity for roaming service in ubiquitous networks. Security and Communication Networks 9(17):4192–4209
3. Karuppiah M, Pradhan A, Kumari S, Amin R, Rajkumar S, Kumar R (2017) Security on "secure remote login scheme with password and smart card update facilities,". International Conference on Mathematics and Computing. Springer, Manhattan
4. Zuowen T (2013) An efficient biometrics-based authentication scheme for telecare medicine information systems. Network 2(3):200–204
5. Yan X, Li W, Li P, Wang J, Hao X, Gong P (2013) A secure biometrics-based authentication scheme for telecare medicine information systems. J Med Syst 37(5):9972
6. Xin X, Zhu P, Wen Q, Jin Z, Zhang H, He L (2013) A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems. J Med Syst 38(1):9994
7. Islam SH, Khan MK (2014) Cryptanalysis and improvement of authentication and key agreement protocols for telecare medicine information systems. J Med Syst 38(10):135
8. Sahoo SS, Mohanty S, Majhi B (2020) A secure three factor based authentication scheme for health care systems using IoT enabled devices. J Ambient Intell Humaniz Comput 12:1419–1434
9. Xue K, Hong P, Ma C (2014) A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture. J Comput Syst Sci 80(1):195–206
10. 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):78
11. Mishra D, Mukhopadhyay S, Chaturvedi A, Kumari S, Khan MK (2014) Cryptanalysis and improvement of Yan et al.'s biometric-based authentication scheme for telecare medicine information systems. J Med Syst 38(6):24
12. Farash M, Turkanović M, Kumari S, Hölbl M (2016) An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. Ad Hoc Netw 36:152–176
13. Almuhaideb AM, Alqudaihi KS (2020) A lightweight and secure anonymity preserving protocol for WBAN. IEEE Access 8(178):183–178,194
14. Das AK (2017) A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor. Int J Commun Syst 30(1):e2933
15. Wu F (2016) An improved and provably secure three-factor user authentication scheme for wireless sensor networks. Peer Peer Netw Appl 11:1–20
16. Jiang Q, Zeadally S, Ma J, He D (2017) Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. IEEE Access 5:3376–3392
17. Amin R, Kumar N, Biswas GP, Iqbal R, Chang V (2018) A light weight authentication protocol for iot-enabled devices in distributed cloud computing environment. Future Generation Comput Syst 78:1005–1019
18. Jia X, He D, Li L, Choo KKR (2018) Signature-based three-factor authenticated key exchange for internet of things applications. Multimed Tools Appl 77(14):18355–18382

19. Zhang L, Zhang Y, Tang S, Luo H (2018) Privacy protection for e-health systems by means of dynamic authentication and three-factor key agreement. IEEE Trans Ind Electron 65:2795–2805
20. Aghili S, Mala H, Shojafar M, Peris-Lopez P (2019) LACO, Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT. Future Gener Comput Syst 96:410–424
21. Chatterjee K (2020) An improved authentication protocol for wireless body sensor networks applied in healthcare applications. Wireless Pers Commun 111(4):2605–2623
22. Lee H, Kang D, Ryu J, Won D, Kim H, Lee Y (2020) A three-factor anonymous user authentication scheme for internet of things environments. J Inf Secur Appl 52:102494
23. Chang YF, Tai WL, Hou PL, Lai KY (2021) A secure three-factor anonymous user authentication scheme for Internet of Things environments. Symmetry 13:1121
24. Yang Z, Lai J, Sun Y, Zhou J (2019) A novel authenticated key agreement protocol with dynamic credential for WSNs. ACM Trans Sens Netw 15(2):22.1-22.27
25. Zhou L, Li X, Yeh KH, Chunhua S, Chiu W (2019) Lightweight IoT based authentication scheme in cloud computing circumstance. Future Gener Comput Syst 91:244–325
26. Turkanović M, Brumen B, Hölbl M (2014) A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks based on the internet of things notion. Ad Hoc Netw 20(96):112
27. Amin R, Biswas GP (2015) An improved rsa based user authentication and session key agreement protocol usable in tmis. J Med Syst 39(8):79
28. Irshad A, Sher M, Nawaz O, Chaudhry SA, Khan I, Kumari S (2017) A secure and provable multi-server authenticated key agreement for TMIS based on Amin et al. scheme. Multimed Tools Appl 76(15):16463–16489
29. Dodis Y, Reyzin L, Smith A (2004) Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In Advances in Cryptology-EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004. Proceedings 23 (pp. 523-540). Springer Berlin Heidelberg.

Publisher's Note

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