Human-centric Computing and Information Sciences

July 2026 | Volume 16

KCIA
Korea Computer Industry Association

www.hcisjournai.com

HCIS | Human-centric Computing and Information Sciences

RESEARCH (Research Manuscript) Open Access

Human-centric Computing and Information Sciences (2026) 16:39
DOI: https://doi.org/10.22967/HCIS.2026.16.039
Received: April 22, 2025; Accepted: July 25, 2025; Published: July 15, 2026

Blockchain-Based Lightweight Anonymous Authentication Scheme for Security Enhancement in Internet of Medical Things Environment

Zaid Ameen Abduljabbar[1,2,3,*], Vincent Omollo Nyangaresi[4,5], Mohammed Abdulridha Hussain[1], Junchao Ma[2,6,*], Mustafa A. Al Sibahee[7], Zaid Alaa Hussien[8], Abdulla J.Y. Aldarwish[1], Ali Hasan Ali[9,10,11], Ahmed Ali Ahmed[7], and Husam A. Neamah[12]

Abstract

The Internet of Medical Things (IoMT) has continued to revolutionize the healthcare sector, resulting in reduced costs and improved quality of treatment. To facilitate real-time remote patient monitoring, biosensors frequently interact with medical systems over the public Internet. This connectivity, however, exposes the IoMT environment to a myriad of privacy and security threats. Although past research has proposed numerous security techniques to address these challenges, most of these solutions fail to provide an adequate balance between security and performance. In this paper, we propose a robust IoMT security scheme that leverages elliptic curve cryptography and one-way hashing operations to achieve low communication, energy, and computation overhead. Formal security analysis using a random oracle model demonstrates the robustness of the negotiated session keys. In addition, semantic security analysis confirms that our scheme mitigates various typical IoMT cyber threats, such as desynchronization, forgery, impersonation, and ephemeral secret leakage attacks. A comparative performance evaluation verifies that the proposed protocol incurs the lowest execution, energy, and communication costs. Specifically, it reduces computation and energy costs by 19.04%, increases supported functionalities by 69.23%, and lowers communication overheads by 8.7%. These efficiencies make our scheme ideal for deployment in IoMT devices with limited energy, processing and communication capabilities.

Keywords

IoMT, Security, Authentication, ECC, Privacy, Biosensor

***Corresponding Author:** Zaid Ameen Abduljabbar (zaid.ameen@uobasrah.edu.iq), Junchao Ma (majunchao@sztu.edu.cn)
[1]Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq
[2]Guangdong Laboratory of Artificial Intelligence and Digital Economy (SZ), Shenzhen, China
[3]Department of Business Management, Al-Imam University College, Balad, Iraq
[4]Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science & Technology, Bondo, Kenya
[5]Department of Applied Electronics, Saveetha School of Engineering, SIMATS, Chennai, Tami lnadu, India
[6]School of Artificial Intelligence, Shenzhen Technology University, Shenzhen, China.
[7]Department of Management and Marketing, College of Industrial Management for Oil and Gas, Basrah University for Oil and Gas, Basrah, Iraq
[8]Information Technology Department, Management Technical College, Southern Technical University, Basrah, Iraq
[9]Department of Mathematics, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq
[10]Technical Engineering College, Al-Ayen University, Thi-Qar, Iraq
[11]Institute of Mathematics, University of Debrecen, Debrecen, Hungary
[12]Department of Electrical Engineering and Mechatronics, Faculty of Engineering, University of Debrecen, Debrecen, Hungary

1. Introduction

The Internet of Medical Things (IoMT) environment is comprised of smart devices and various interconnected systems that collect, process and transmit health-related data [1]. These systems include portable health applications, wearable or implantable biosensors and remote monitoring systems [2]. The physiological data continuously collected by these biosensors include heart rate, electrocardiography, respiratory rate, blood pressure, oxygen saturation, electromyography, body temperature, glucose levels, electroencephalography and electrocardiogram. Data such as patient movement, activity, sleep patterns, posture and medication adherence can also be collected [3, 4]. These data are collected in real-time and shared with medical experts for appropriate intervention. At the patient's end, a control unit such as a smartphone can be incorporated to amalgamate healthcare data from various sensors and forward it to other devices. This control unit can also serve as a gateway between the hospital servers and patient sensors. The analysis of these data can facilitate early disease diagnosis, personalized treatment and the initiation of corrective responses [5–7].

The integration of biosensors with medical equipment and electronic health records enables healthcare professionals to remotely monitor patients in real time, make informed decisions, take proactive responses and administer individualized treatment [8–10]. Therefore, the IoMT has improved the healthcare sector in areas such as chronic diseases management, healthcare accessibility, drug adherence, reduced expenses, increased patient engagement, enhanced healthcare quality and effective personalized treatment [11–13]. Reductions in healthcare costs are enabled by the remote monitoring of patients in their homes [14]. This also helps decongest hospitals and reduce the medical staff's workload. As explained in [15], significant benefits of the IoMT include decreased error rates, improved patient experience and increased treatment efficiencies. Once the data are forwarded to medical servers (MSs), machine learning algorithms and advanced analytics can be deployed to gain critical insights that facilitate preventative interventions.

The IoMT has revolutionized the healthcare sector through data-driven personalized treatments and real-time remote monitoring of patients. To facilitate this real-time data exchange between biosensors and hospital servers, frequent interactions occur over the insecure public Internet. This raises numerous security and privacy challenges regarding the sensitive patient data transmitted in these networks [16–19]. Any successful data breach or network intrusion can have serious repercussions, including the loss of life. Some of the cyber threats in the IoMT include unauthorized access, tracking, smart card theft, physical sensor capture, session key leakages, desynchronization, hacking, denial-of-service (DoS) attack, forgery, eavesdropping, man-in-the-middle (MitM) attack and privileged insider attacks [20, 21]. In addition, attackers can intercept communication between medical sensors and hospital systems to steal or alter the transmitted data. This compromises the privacy of sensitive patient records, and malicious modifications can result in misdiagnosis. This can lead to inappropriate drug administration, which can endanger a patient's life [22].

To address the security and privacy threats in the IoMT, strong authentication techniques must be implemented. Therefore, many authentication protocols have been presented in the recent past to maintain the confidentiality and integrity of transmitted data. However, due to their limited storage, communication and processing capabilities, IoMT biosensors are unable to execute highly sophisticated cryptographic procedures.

1.1 Motivation

The healthcare sector has seen an increase in cyber-attacks in the recent past. According to the European Union Agency for Network and Information Security, a 55% increase in these attacks occurred in 2023, frequently targeting IoMT devices. A significant number of these devices have vulnerabilities, which have been exploited in 41%–88% of attacks. A report by the Science and Information Organization indicates that over 6.2% of IoMT devices have been impacted by ransomware, which has cost organizations millions of dollars. This report also indicates that 53% of critical healthcare systems have

been affected, leading to loss of patient records and costing more than $22 million. Therefore, addressing these security challenges is critical. However, the majority of current solutions are characterized by either high complexity or security lapses that can still be exploited to wreak havoc in the IoMT. As a result, robust IoMT security is needed at a low cost.

1.2 Contributions

IoMT sensors and medical systems have continued to positively affect the healthcare sector by facilitating patient data management and remote, real-time patient monitoring. However, these networks have also introduced numerous security and privacy threats and vulnerabilities to sensitive patient data [23]. Therefore, the IoMT needs to be protected from malicious intrusions and other cyber threats. Although numerous security solutions have been developed recently, the majority of them are inefficient for the resource-constrained IoMT smart devices. Robust security protocols often require high computation and communication capabilities, which can drain sensor batteries in a very short time [24]. In addition, the IoMT environment is highly dynamic, with smart devices frequently leaving and joining the network. This highlights a need for efficient authentication and key management schemes. In light of this, this paper makes the following major contributions:

- We incorporate a decentralized private blockchain (*BC*) in the registration process to mitigate threats from privileged insider attacks and single points of failure, which are inherent in centralized security protocols. This contrasts with most current schemes where registration is centrally executed by a trusted or registration authority.
- To eliminate human errors, our protocol executes authentication without human intervention. This helps reduce authentication errors often found in current password- and biometrics-based schemes.
- We include location data in authentication procedures to mitigate physical attacks, such as stolen sensors. This ensures that sensors stolen from one location cannot be deployed elsewhere.
- To reduce communication overhead, our protocol executes mutual authentication without involving gateway nodes (*GWN*s) or a trusted authority (*TA*).
- We carry out elaborate formal and informal security analyses to demonstrate the robustness of the negotiated session keys and our protocol against typical IoMT attacks, respectively.
- An extensive comparative performance evaluation shows that our protocol incurs the lowest computation, energy and communication costs.

1.3 Threat Model

The Canetti–Krawczyk (CK) model is a well-known framework for depicting the attacker capabilities in most authentication protocols. In this model, we assume that message exchanges between biosensors and hospital MSs occur over the open public Internet. As such, attackers can intercept, eavesdrop on and retrieve sensitive data from communication channels. Specifically, the adversary $\tilde{A}$ is capable of:

- Intercepting and altering the messages exchanged between biosensors and MSs;
- Replaying old but valid messages to unsuspecting IoMT entities;
- Physically capturing the biosensors and other IoMT elements and extract stored security tokens via power analysis techniques;
- Brute-forcing and performing guessing to disclose the deployed security keys;
- Composing and inserting malicious messages in the IoMT environment;
- Repudiating all transmitted messages;
- Tracking IoMT entities and associating captured messages to particular parties.

1.4 Requirements

Data origin authentication: MSs must verify the origin of all received data to prevent the insertion of

malicious data into the communication channel. This is achieved through the use of regional codes generated during the registration phase.

Patient records confidentiality: Collected data forwarded to MSs must be kept confidential due to its sensitive nature. This confidentiality is enabled by negotiated session keys, which are used to encrypt data transmitted across the public Internet.

Sensor data integrity and authorization: Data forwarded from sensors to MSs must be protected against malicious modifications. Therefore, strong mutual authentication must be executed before servers can accept or access the data.

Uninterrupted accessibility and availability: Sensors on the patient side should frequently forward real-time patient data to MSs without interruption. To ensure this, DoS and desynchronization threats must be mitigated.

Non-repudiation and conditional privacy: All IoMT participants should be capable of being positively identified by a TA. In addition, the TA should be capable of associating these network entities to their messages when necessary.

Data freshness: Data transmitted from sensors to MSs should be up to date to facilitate relevant decision-making and interventions. Therefore, malicious data interception, modifications and forwarding should be mitigated. This can be achieved by incorporating timestamps in all exchanged messages.

Efficiency and attack resiliency: Long latencies are discouraged in the IoMT due to the time-sensitive nature of the data. Delays in the proper reception of sensory data can postpone critical decisions and interventions, potentially leading to a loss of patient life. Moreover, malicious entities and activities should be prevented to mitigate fatalities that can result from cyber-attacks.

The remainder of this paper is structured as follows. Section 2 discusses related authentication protocols, and Section 3 presents the proposed scheme. Section 4 provides the security analyses of our scheme, and Section 5 details its performance evaluation. Finally, Section 6 offers a conclusion and outlines future research scopes in this domain.

1.5 Mathematical Preliminaries

Our scheme deploys elliptic curve cryptography (ECC) because of its robust security with relatively short key sizes, especially when compared to other public key-based techniques, such as RSA (Rivest–Shamir–Adleman). In addition, we use a collision-resistant one-way hashing function due to its efficiency and the difficulty of reversing it. The mathematical formulations for ECC and the hashing function are described in the sections that follow.

1.5.1 ECC

Let s and t be constants and P be a base point of the elliptic curve $E_p^*(s,t)$ over some finite field denoted by F_p^*, where p is a large prime number. We also let $(x,y) \in z_p^* \times z_p^*$ be a set of solutions to congruence denoted by Equation (1):

$$y^2 \equiv x^3 + sx + t \ (mod\ p) \tag{1}$$

Considering the Galois field (GF), the elliptic curve $E_p^*(s,t)$ over $GF(p)$ is defined as in Equation (2):

$$y^2 = x^3 + sx + t \tag{2}$$

The security of this elliptic curve emanates from the discrete logarithm problem in a group that is defined by the various points on this elliptic curve. On this curve, $s,t \in GF(p)$ must satisfy Equation (3):

$$4s^3 + 27t^2 \neq 0 \ (mod\ p) \tag{3}$$

The difficulty of the elliptic curve discrete logarithm (ECDL) problem is critical for the security of all ECC-based protocols. Specifically, the elliptic curve Diffie–Hellman (ECDH) problem and ECDL mathematical problems are crucial in these security protocols. The definitions of these problems are as follows.

ECDL problem: Given elliptic curve $E_p^*(s,t)$ defined over $GF(p)$ and two points $U, V \in E_p^*(s,t)$ whose order is q, finding integer $i \in z_q^*$, such that $U = i.P$, is computationally challenging.

ECDH problem: Suppose that P is the generator of a cyclic group G of prime order on $E_p^*(s,t)$. We let a and b be two points, such that $a, b \in z_q^*$. Suppose that aP, bP and P are known. However, deriving abP in polynomial time τ remains infeasible.

1.5.2 Hashing function

The difficulties of reversing the one-way hashing function rely on its pre-image and collision-resistance.

First pre-image resistance: Consider hash function $h: \{0,1\}^* \rightarrow \{0,1\}^s$ and the following hash value:

$$y = h(x) \tag{4}$$

The adversary's interest is to find input x^*, such that

$$h(x^*) = y \tag{5}$$

Mathematically, finding x^* is equivalent to a brute force search over 2^s possibilities. However, no algebraic structure can efficiently solve $h(x^*) = y$.

Second pre-image resistance: Given input p, finding another input q is extremely difficult, such that

$$h(p) = h(q) \tag{6}$$

This is attributed to the hash function's avalanche effect, which serves to mitigate targeted collisions. Due to the stochastic nature of $h(.)$, any small change in input p results in extremely large capricious change in $h(p)$, thereby complicating any practical systematic searches.

Collision-resistance: Suppose that z_1 and z_2 are two inputs to the hashing function. Given $z_1 \neq z_2$, the following is difficult to find:

$$h(z_1) = h(z_2) \tag{7}$$

Consider a k-bit hash function. Using a generic birthday attack, finding a collision requires $2^{\frac{k}{2}}$ operations. However, hash functions are characterised by high entropies, and k is normally a large value, thereby rendering collision attacks extremely infeasible.

2. Related Works

The need to provide security for information exchanged in the IoMT has led to the development of various authentication techniques. For instance, biometrics-bases authentication techniques are presented in [25–29]. Although biometrics technology enhances IoMT security, it requires additional hardware that can hinder seamless integration. In addition, these schemes need extensive fuzzy extraction procedures that can lead to high processing costs [30]. Moreover, the protocol in [27] cannot withstand threats from a stolen controller device [31]. Likewise, a zero-trust deployment model is presented in [32], but it has not been evaluated against security threats, such as side-channelling and session-hijacking. To provide enhanced IoMT security, protocols based on ECC have been developed in [33–35]. However, the scheme in [34] suffers from numerous security challenges [36], and the protocol in [33] requires extensive scalar point multiplications, resulting in high computation overheads [37]. To address the security issues in [34], an improved scheme is introduced in [38]. Unfortunately, a cryptanalysis by [36] reveals many security vulnerabilities in [38]; hence, an enhanced technique is developed in [35]. However, this improved scheme is vulnerable to ESL attacks [33].

To overcome computational inefficiencies in [33], the identity-based lightweight scheme developed by [39] can be utilized. However, identity-based protocols are susceptible to key escrow challenges. In addition, this protocol fails to provide perfect anonymity amongst biosensors due to inefficient digital

signature management for each device [36]. As a result, improved anonymous authentication approaches are introduced in [29, 40, 41]. Although the scheme in [29] achieves forward security and resistance against MitM and insider attacks, its use of numerous fuzzy extractions results in high processing overheads. Conversely, the technique in [40] is susceptible to master secret compromise, ESL, impersonation and key compromise threats [31]. Similarly, the protocol in [41] protects against smart card loss but remains vulnerable to tampering and physical attacks [42]. To address these issues, an enhanced certificate-based scheme is introduced in [43]. Although this protocol supports privacy, integrity and resistance against replay threats, its certificate management may not scale well with increased network entities. In addition, it fails to provide anonymity and joint validation [31].

Consequently, numerous certificate-less authentication techniques are presented in [17, 44–49]. The authors in [36] note that security and performance evaluations are missing in [48]. The identity-based scheme in [17] is prone to key escrow challenges [50]. Protocols that rely on extensive point multiplications, such as those in [44, 46, 49], and bilinear pairing operations [45, 49, 51] often incur significant computation costs. For example, the execution time for [49] is long due to its use of bilinear pairing during partial private key distribution, and it also lacks forward key secrecy and protection against replays [31]. Similarly, the ECC-based protocol in [52] is not evaluated against attacks such as desynchronization, session hijacking and side-channelling, and its scalar multiplication operations result in high computation costs. Physically unclonable function (PUF)-based techniques, such as those in [47, 57, 58], are also characterized by instability challenges. Although [58] is a batch authentication technique, it fails to offer anonymity and untraceability [42]. To address these issues, lightweight authentication techniques are introduced in [53–55]. However, the scheme in [53] is susceptible to desynchronization attacks [42]. The protocol in [54] is also vulnerable to desynchronization and session key disclosure attacks and lacks forward key security [42, 56]. Additionally, the protocol in [55] cannot support anonymous communication [42]. A more improved authentication approach is introduced in [59], but while it preserves anonymity, its extensive point multiplications make it computationally inefficient.

Based on this discussion, the provision of perfect security at low computation, energy and communication costs is extremely elusive. Despite numerous efforts from academia and industry, most presented schemes remain vulnerable to various security attacks, and others are computationally inefficient. The proposed scheme, however, is shown to mitigate most typical IoMT security threats while incurring minimal computation, energy and communication overheads.

3. The Proposed Scheme

The main network elements in our scheme include the *TA*, an *MS*, a sensor unit (*SU*) and a *GWN*. The *SU* is implanted in the patient's body or placed in the vicinity of the patient to collect physiological data. The *GWN* interconnects the *SU* to the *MS*, which stores all the collected patient data. The *TA* registers all the *SUs* and *MSs* and is assumed to be sufficiently secured. Fig. 1 presents the network model of the proposed scheme.

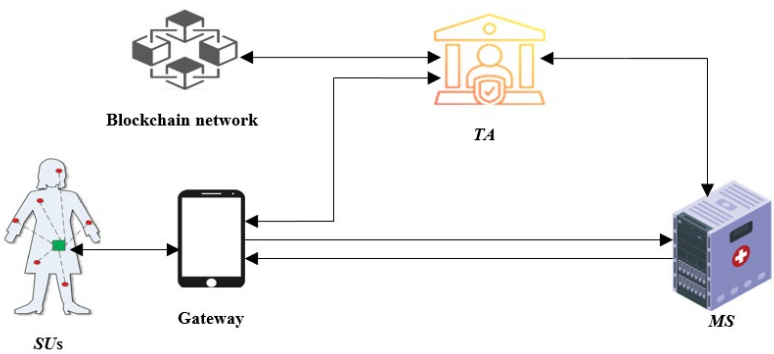

Fig. 1. Network model.

In terms of operations, our protocol comprises of four main phases: system initialization, registration, authentication, and dynamic sensor addition. Registration takes place over secured channels, and authentication and session key negotiation are performed across public channels. Table 1 presents the notations utilized throughout this paper.

The subsections below describe of the various phases of our proposed scheme.

Table 1. Notations

Symbol	Description
TA	Trusted authority
MS_j	Medical server j
GWN	Gateway node
SU_i	Sensor unit i
h (.)	One-way hashing function
$\|\|$	Concatenation operation
$\oplus$	XOR operation
G_{pk}, G_{sk}	Public and private keys belonging to GWN, respectively
ID_{TA}	Unique identity of the TA
ϕ, a_c	Private and public keys for TA, respectively
SID_i	Unique identity for sensor unit SU_i
GID	Unique identity of GWN
MID_j	Unique identity of MS_j
RC_i, RC_j	Regional codes for SU_i and MS, respectively
T_i	ith timestamp
ΔT	Maximum transmission delay
ΔR	Location threshold
SK_{ms}	Session key derived at MS
E_k/D_k	Encrypt and decrypt using k, respectively

3.1 System Initialization

The essence of this phase is for the TA to distribute private tokens to the sensor nodes and MS via the BC. As such, the BC ledger keeps records of the identities of all MSs and sensor nodes. The specific steps followed during the system initialisation are described below.

Step 1: The TA selects an ECC base point P. It also chooses the GWN's unique identity GID and private key G_{sk}, as shown in Fig. 2. Next, it computes the corresponding GWN public key as $G_{pk} = P.G_{sk}$.

Step 2: The TA chooses a one-way hashing function h(.). At the end, it publishes $\{G_{pk}, h(.), P, E^*_p (s, t)\}$, where (s, t) are constants.

3.2 Registration

In this phase, the TA registers itself to the BC network. Thereafter, the SUs and MSs are also registered to the BC via the TA. During this process, some security tokens are loaded unto the SUs prior to their actual field deployment. The following subsections describe the registration process in some greater details.

3.2.1 TA registration

In this phase, the TA registers itself with the BC. Afterwards, the TA uploads the SUs' identity data into the BC. The following two steps are critical during this registration process.

Step 1: The TA selects a random nonce r_1 and generates its unique identity ID_{TA}.

Step 2: The TA derives $a_b = h\ (r_1.P||ID_{TA})$. Next, it composes $BC_a = \{a_b, h\ (ID_{TA})\}$ and forwards it to the BC network for storage. Finally, the TA keeps $\{r_1, ID_{TA}\}$ as secret parameters.

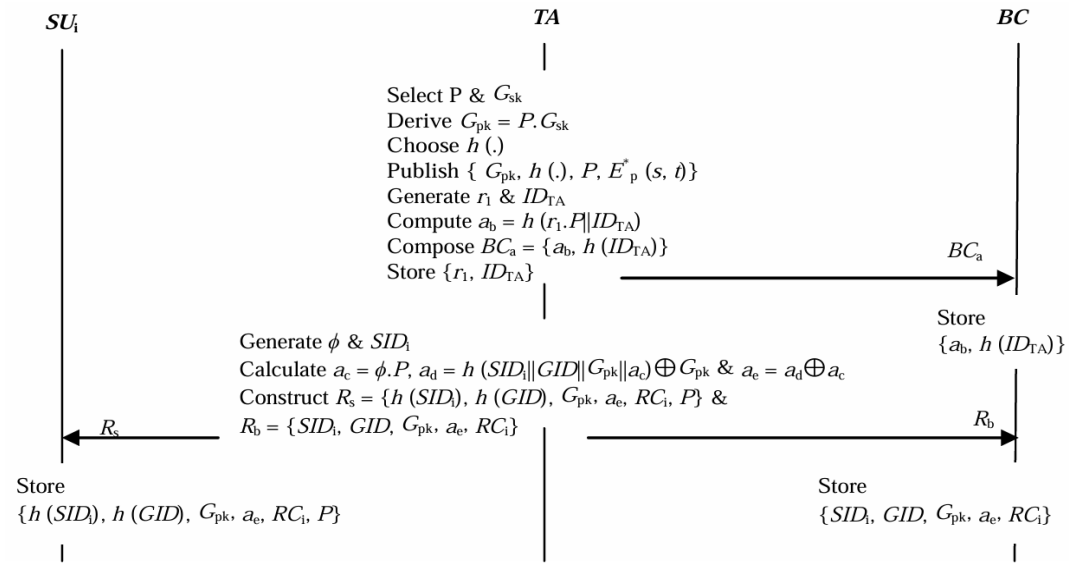

Fig. 2. System initialization and registration.

3.2.2 SU registration

In this phase, the sensor nodes are registered at the *TA* via the *BC*. The following two steps are followed during this registration process.

Step 1: The *TA* generates some private keys ϕ. Next, it chooses a unique identity SID_i for the SU_i. It then derives $a_c = \phi.P$, $a_d = h\ (SID_i||GID||G_{pk}||a_c) \oplus G_{pk}$ and $a_e = a_d \oplus a_c$.

Step 2: The *TA* constructs $R_s = \{h\ (SID_i), h\ (GID), G_{pk}, a_e, RC_i, P\}$ and forwards it to the SU_i where these values are stored in memory. Finally, the *TA* forwards $R_b = \{SID_i, GID, G_{pk}, a_e, RC_i\}$ to the *BC* for storage.

The above two steps are followed to register the *MS*. Therefore, the *MS* stores $\{h\ (MID_j), h\ (GID), G_{pk}, b_e, RC_j, P\}$ in its repository upon successful registration.

3.3 Authentication and Key Setup

In this phase, the SU and MS mutually authenticate each other and set up a session key deployed for secure data exchange. Fig. 3 presents a high-level overview of the authentication flow. This authentication and key agreement are facilitated by the secret tokens already preloaded during the registration phase. The following six steps are executed during this process.

Step 1: The SU_i generates a random nonce r_2 at timestamp T_1. Next, it derives $b_a = h\ (h(SID_i)||h(GID)||G_{pk}||T_1) \oplus a_e$, $b_c = h\ (h(GID)||G_{pk}||T_1||a_e) \oplus r_2.P$ and $b_d = h\ (h(GID)||r_2.P||a_e) \oplus RC_i$. At the end, it constructs a message $auth_a = \{h(SID_i), b_a, b_c, T_1, b_d\}$, which is forwarded to the *MS*, as shown in Fig. 4.

Step 2: Upon receiving the message $auth_a$, the *MS* establishes the current timestamp T_2 and checks whether $T_2 - T_1 \leq \Delta T$, where is the maximum permissible transmission latency. If this condition does not hold, then the authentication session is terminated. Otherwise, the *MS* recomputes $a_e^* = h\ (h(SID_i)||h(GID)||G_{pk}||T_1) \oplus b_a$.

Step 3: The *MS* derives $r_2.P^* = h\ (h(GID)||G_{pk}||T_1||a_e^*) \oplus b_c$ and $RC_i^* = h\ (h(GID)||\ r_2.P^*||a_e^*) \oplus b_d$. This is the determination of whether $RC_j - RC_i \leq \Delta R$, such that the session is halted if this condition does not hold. Otherwise, the *MS* generates a random nonce r_3 at timestamp T_3.

Step 4: The *MS* computes $b_e = r_3(r_2.P^*)$, $c_a = h\ (a_e||r_2.P^*\ ||G_{pk}||h(MID_j)||h(GID)||T_3) \oplus b_e$, $c_b = h\ (b_e||G_{pk}||\ h(MID_j)||T_3) \oplus r_3$, $c_d = h\ (h(GID)||r_3||b_e) \oplus RC_j$ and session key $SK_{ms} = h\ (h(SID_i)||h(MID_j)||h(GID)||$

$G_{pk}||b_e||r_2.P^*||T_1||T_3||RC_i^*||RC_j$). Finally, the *MS* composes a message $auth_b = \{h(MID_j), c_a, c_b, T_3, c_d\}$, which is passed across to the SU_i.

Step 5: On getting the message $auth_b$, the SU_i determines the present timestamp T_4. Next, it checks if $T_4 - T_3 \leq \Delta T$, halting the session upon verification failure. Otherwise, it recomputes $b_e^* = h\ (a_e||r_2.P^*||G_{pk}||h(MID_j)||h(GID)||T_3) \oplus c_a$, $r_3^* = h\ (b_e^*||G_{pk}||h(MID_j)||T_3) \oplus c_b$ and $RC_j^* = h\ (h(GID)||r_3^*||b_e^*) \oplus c_d$.

Step 6: The SU_i confirms whether $RC_i - RC_j^* \leq \Delta R$. Basically, the session is terminated if this condition does not hold. Otherwise, the SU_i calculates $b_e^* = r_3^*\ (r_2.P)$, as well as session key $SK_{sm} = h\ (h(SID_i)||h(MID_j)||h(GID)||G_{pk}||b_e^*||r_2.P||T_1||T_3||RC_i^*||RC_j^*)$. Finally, the *MS* and SU_i set $SK_{sm} = SK_{ms}$ as the session key for encrypting the data exchanged over insecure wireless channels.

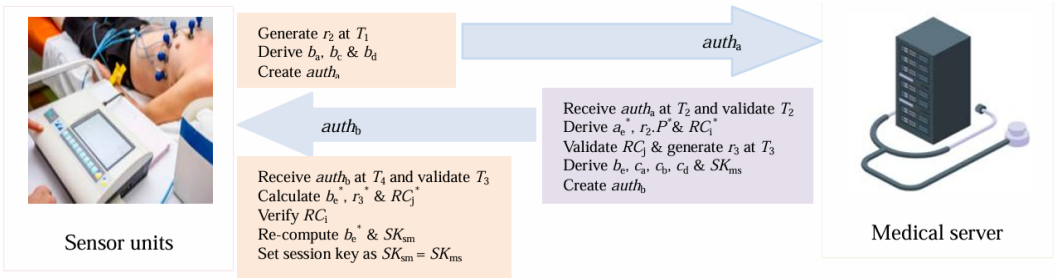

Fig. 3. High-level overview of the authentication flow.

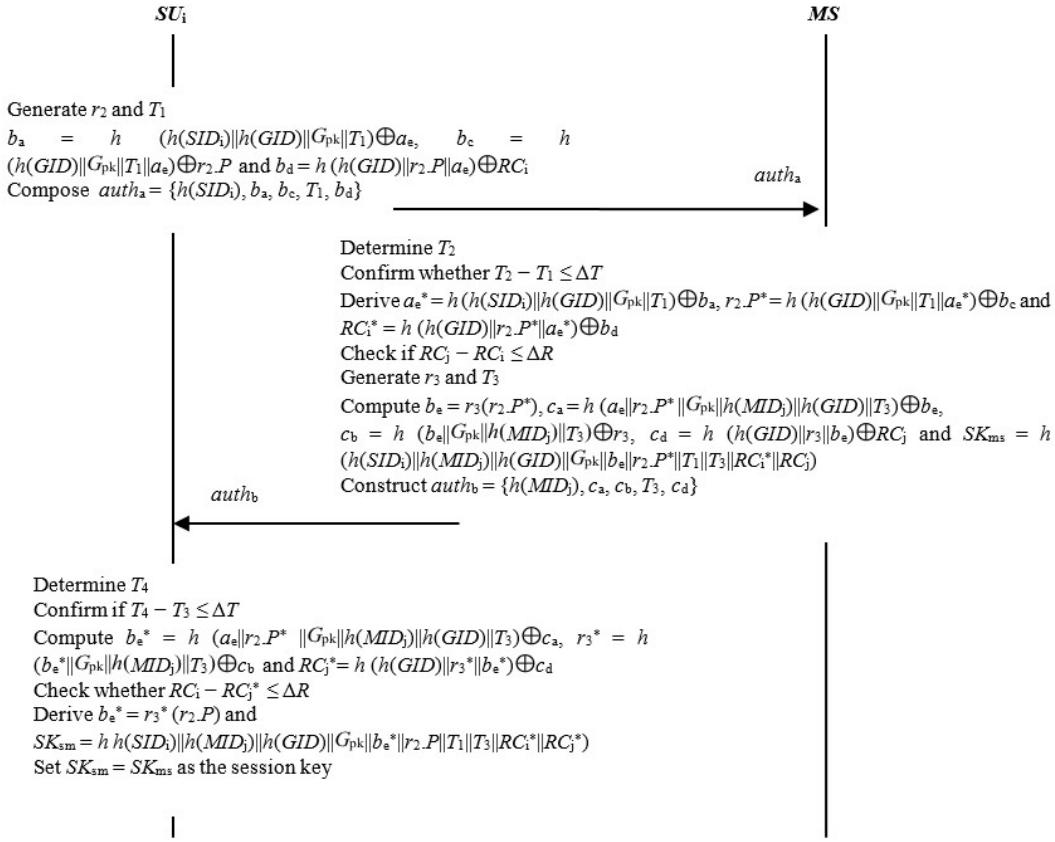

Fig. 4. Authentication and session key agreement.

3.4 Dynamic Sensor Addition

This phase is activated whenever the *SU*s fail, malfunction, are stolen or are lost. To facilitate continuous remote patient monitoring, new *SU*s must be added through the following steps.

Step 1: The *TA* generates its private key ϕ and selects *SU* identity SID_i. Next, it derives $a_c = \phi.P$, $a_d = h(SID_i||GID||G_{pk}||a_c) \oplus G_{pk}$ and $a_e = a_d \oplus a_c$.

Step 2: The *TA* constructs a message $Reg = \{h(SID_i), h(GID), G_{pk}, a_e, RC_i, P\}$ and forwards it towards the SU_i over secure communication channels. Finally, TA sends $\{SID_i, GID, G_{pk}, a_e, RC_i\}$ to the *BC* for storage.

Step 3: Upon receiving *Reg* from *TA*, the SU_i stores $\{h(SID_i), h(GID), G_{pk}, a_e, RC_i, P\}$ in its memory.

4. Security Analysis

In this section, we present formal and informal security analyses of the proposed scheme. The sub-sections that follow gives detailed description of these analyses.

4.1 Formal Security Analysis

In this subsection, we utilise the well-known random oracle model (ROM) to demonstrate the robustness of the negotiated session keys SK_{ms} and SK_{sm}. We demonstrate that the session keys are still secure even if the attacker has access to secret values for the *SU* $\{SID_i, GID, a_e, RC_i, \phi, G_{sk}\}$, as well as the security token for the *MS* $\{MID_j, GID, G_{sk}, b_e, RC_j, \phi\}$. To accomplish this, the oracle is assumed to successfully execute Query 1 and Query 2, as described below.

Query 1: The oracle can deploy this *reveal* () query to obtain a hash message *m* from some hash outputs λ, where $\lambda = h(m)$.

Query 2: Given the elliptic curve base point $P \in E_p(s,t)$, the oracle can derive the secret key *k* from its corresponding public key *K*, where $K = k \times P$.

Lemma 1: Assume that the hash function and ECDH act as the ROM. In addition, let the adversary $\tilde{A}$ utilise power analysis techniques to extract values $\{h(SID_i), h(GID), G_{pk}, a_e, RC_i, P\}$ and $\{h(MID_j), h(GID), G_{pk}, b_e, RC_j, P\}$ stored in SU_i and *MS*, respectively. However, the adversary $\tilde{A}$ cannot retrieve $\{SID_i, \phi, GID\}$ from the SU_i.

Proof: Suppose that attacker the adversary $\tilde{A}$ has access to values $\{h(SID_i), h(GID), G_{pk}, a_e, RC_i, P\}$ stored in the SU_i's memory via side-channelling. In addition, assume that the adversary $\tilde{A}$ can correctly guess $\{SID_i, \phi, GID\}$. Next, the attacker proceeds to verify the authenticity of the guessed values. To accomplish this, the adversary $\tilde{A}$ derives $G_{pk} = P.G_{sk}$, $a_e = a_d \oplus a_c$, where $a_d = h(SID_i||GID||G_{pk}||a_c) \oplus G_{pk}$ and $a_c = \phi.P$. This is followed by the deployment of *Query 1* as input to oracle $h(SID_i)$, that is,

$$SID_i \leftarrow Query\ 1\ (h(SID_i)).$$

Similarly, Query 1 is utilised as an input to oracle $h(GID)$, as evidenced as follows:

$$GID \leftarrow Query\ 1\ (h(GID)).$$

To retrieve G_{sk}, *Query* 2 is deployed as input to oracle G_{pk} as follows:

$$G_{sk}.P \leftarrow Query\ 2\ (G_{pk}).$$

Thereafter, the adversary $\tilde{A}$ derives $h(SID_i^*)$, $h(GID^*)$, $G_{pk}^* = P.G_{sk}^*$ and $a_e^* = a_d^* \oplus a_c^*$. The adversary then checks if $G_{pk}^* = G_{pk}$, returning a failure if this condition does not hold; otherwise, success is returned. Next, the adversary $\tilde{A}$ determines if $a_e^* = a_e$, returning failure when this condition does not hold; otherwise, success is returned. Thereafter, the adversary $\tilde{A}$ computes SID_i, ϕ and *GID* for SU_i and *MS*.

We denote the success probability as *Pr* (.). Therefore, the success probability that the adversary $\tilde{A}$ has

in breaking the ECDH and h (.) is denoted as $Pr\,[\tilde{A}^{ECDH\_h}]$. As such, the function of $Pr\,[\tilde{A}^{ECDH\_h}]$ is denoted as $Succ = |Pr\,[\tilde{A}^{ECDH\_h} = 1] - 1|$. In addition, we represent the advantage function for $Pr\,[\tilde{A}^{ECDH\_h}]$ as $Adv_{\tilde{A}}(t_r, q_n) = max\,(Succ)$, where t_r is the running time, and q_n is a particular query n launched by the adversary $\tilde{A}$. Moreover, let μ be a small value, such that $\mu > 0$. The proposed protocol is safe against threats posed by the adversary $\tilde{A}$ on the condition that $Adv_{\tilde{A}}(t_r, q_n) \leq \mu$. Suppose that the adversary $\tilde{A}$ is interested in retrieving values protected by h (.) and ECDH, such as SID_i, GID and ϕ. However, accessing security tokens protected by ECDH and h (.) is mathematically infeasible. As such, the adversary $\tilde{A}$ cannot extract $\{SID_i, GID, \phi\}$.

Lemma 2: Suppose that ECDH and h (.) are inputs to the random oracle. In addition, we assume that the adversary $\tilde{A}$ has captured values $\{h(SID_i), b_a, b_c, T_1, b_d, h(MID_j), c_a, c_b, T_3, c_d\}$ exchanged in messages $auth_a$ and $auth_b$. However, the adversary $\tilde{A}$ is still unable to derive session keys $SK_{ms} = h\,(h(SID_i)||h(MID_j)||h(GID)||G_{pk}||b_e||r_2.P^*||T_1||T_3||RC_i^*||RC_j)$ and $SK_{sm} = h\,(h(SID_i)||h(MID_j)||h(GID)||G_{pk}||b_e^*||r_2.P||T_1||T_3||RC_i^*||RC_j^*)$.

Proof: Suppose that the adversary $\tilde{A}$ has captured messages $auth_a = \{h(SID_i), b_a, b_c, T_1, b_d\}$ and $auth_b = \{h(MID_j), c_a, c_b, T_3, c_d\}$. In addition, we assume that the adversary $\tilde{A}$ has access to security tokens such as SID_i, ϕ and GID. Thereafter, the adversary $\tilde{A}$ proceeds to derive session keys $SK_{ms} = h\,(h(SID_i)||h(MID_j)||h(GID)||G_{pk}||b_e||r_2.P^*||T_1||T_3||RC_i^*||RC_j)$ and $SK_{sm} = h\,(h(SID_i)||h(MID_j)||h(GID)||G_{pk}||b_e^*||r_2.P||T_1||T_3||RC_i^*||RC_j^*)$. To accomplish this, the adversary $\tilde{A}$ calculates $b_a = h\,(h(SID_i)||h(GID)||G_{pk}||T_1) \oplus a_e$, $b_c = h\,(h(GID)||G_{pk}||T_1||a_e) \oplus r_2.P$, $b_d = h\,(h(GID)||\,r_2.P||a_e) \oplus RC_i$, $c_a = h\,(a_e||r_2.P^*\,||G_{pk}||h(MID_j)||h(GID)||T_3) \oplus b_e$, $c_b = h\,(b_e||G_{pk}||h(MID_j)||T_3) \oplus r_3$ and $c_d = h\,(h(GID)||r_3||b_e) \oplus RC_j$. To retrieve SU identity SID_i, the adversary supplies Query 1 as input to oracle h (SID_i) as follows:

$$SID_i \leftarrow Query\ 1\ (h\ (SID_i)).$$

Similarly, the unique identity of the MS_j (MID_j) is obtained by supplying Query 1 as the input to oracle h (MID_j), as shown as follows:

$$MID_j \leftarrow Query\ 1\ (h\ (MID_j)).$$

This is followed by the derivation of parameters $b_a^* = h\,(h(SID_i^*)||h(GID^*)||G_{pk}^*||T_1) \oplus a_e$, $b_c^* = h\,(h(GID^*)||G_{pk}^*||T_1^*||a_e) \oplus r_2^*.P$, $b_d^* = h\,(h(GID^*)||r_2^*.P||a_e) \oplus RC_i$, $c_a^* = h(a_e||r_2^*.P\,||G_{pk}^*||h(MID_j^*)||h(GID^*)||T_3^*) \oplus b_e$, $c_b^* = h\,(b_e||G_{pk}^*||h(MID_j^*)||T_3^*) \oplus r_3^*$ and $c_d^* = h\,(h(GID^*)||r_3^*||b_e) \oplus RC_j$. Next, the adversary checks if $b_a^* = b_a$, $b_c^* = b_c$, $b_d^* = b_d$, $c_a^* = c_a$, $c_b^* = c_b$ and $c_d^* = c_d$. On the condition that the outcomes of these verifications are negative, failure is returned. Otherwise, the adversary $\tilde{A}$ successfully derives session key $SK_{sm} = SK_{ms}$. Here, the success probability function of this derivation is denoted as $Succ = |Pr\,[\tilde{A}^{ECDH\_h} = 1] - 1|$, whereas the advantage function is represented by $Adv_{\tilde{A}}(t_p, q_s) = max\,(Succ)$, where t_p is the execution time, and q_s is a specific query n initiated by the adversary $\tilde{A}$.

Our protocol is robust against threats posed by the adversary $\tilde{A}$, provided that $Adv_{\tilde{A}}(t_p, q_s) \leq \mu$ for some small values $\mu > 0$. In our scheme, if the adversary $\tilde{A}$ can retrieve security tokens protected with h (.) and ECDH, then the derivation of session key $SK_{sm} = SK_{ms}$ can be attempted. However, extracting values protected by h (.) and ECDH is computationally infeasible. In a nutshell, the adversarial derivation of SK_{sm} and SK_{ms} is infeasible in our scheme due to the difficulties of solving the ECDH problem and reversing the collision-resistant h (.) function.

4.2 Informal Security Analysis

In this subsection, we show that the proposed protocol is sufficiently robust against the attacker capabilities in the CK model. As such, we state and proof the salient features supported by our scheme as detailed below.

Our scheme offers location-aware verification: In wireless networks, adversaries can steal SUs from one location and deploy them elsewhere to commit illicit activities. To address this, our protocol preloads location data into SUs and servers $\{RC_i, RC_j\}$. We also specify a location threshold ΔR that dictates how

far the network entities can be shifted from their initial regions. During the authentication process, these location data are incorporated in the derived transient values. It is therefore infeasible for sensors and servers to be stolen from one region and deployed in other regions.

Eavesdropping and impersonation attacks are mitigated: Suppose that the adversary $\tilde{A}$ is interested in eavesdropping the public challenges and afterwards attempt to impersonate the SU_i or *MS*. For this impersonation to succeed, the adversary $\tilde{A}$ must construct valid messages $auth_a = \{h(SID_i), b_a, b_c, T_1, b_d\}$ and $auth_b = \{h(MID_j), c_a, c_b, T_3, c_d\}$. Here, $b_a = h\,(h(SID_i)||h(GID)||G_{pk}||T_1) \oplus a_e$, $a_e = a_d \oplus a_c$, $a_d = h\,(SID_i||GID||G_{pk}||a_c) \oplus G_{pk}$, $a_c = \phi.P$, $b_c = h\,(h(GID)||G_{pk}||T_1||a_e) \oplus r_2.P$, $c_a = h\,(a_e||r_2.P^*\,||G_{pk}||h(MID_j)||h(GID)||T_3) \oplus b_e$, $c_b = h\,(b_e||G_{pk}||h(MID_j)||T_3) \oplus r_3$ and $c_d = h\,(h(GID)||r_3||b_e) \oplus RC_j$. Evidently, the adversary $\tilde{A}$ must have access to unique identities $\{MID_j, SID_i, GID\}$, random nonces $\{r_2, r_3\}$ and *TA*'s private key ϕ, amongst other values. Given that these values are never exchanged in plain text over the public channels, the adversary $\tilde{A}$ cannot obtain them. Therefore, these two attacks flop.

Anonymity and untraceability are attained: In our protocol, all *SU*s are securely registered to the private *BC* network via the *TA*. Therefore, credentials such as $\{a_b, h\,(ID_{TA})\}$, $\{SID_i, GID, G_{pk}, a_e, RC_i\}$ and $\{MID_j, GID, G_{pk}, a_e, RC_j\}$ are safely stored in the *BC*. During the authentication procedures, messages $auth_a = \{h(SID_i), b_a, b_c, T_1, b_d\}$ and $auth_b = \{h(MID_j), c_a, c_b, T_3, c_d\}$ are exchanged between *MS* and SU_i. Although these messages incorporate unique identities $\{SID_i, MID_j\}$, they are protected by the collision-resistant one-way hashing function. Given that reversing this hashing function is computationally infeasible, anonymity of these unique identities is preserved. Therefore, the adversary $\tilde{A}$ cannot deploy these messages as vectors for tracking *MS* and SU_i.

The developed protocol prevents MitM and forgery attacks: Assume that the adversary $\tilde{A}$ can generate valid timestamps T_1 and T_3. In addition, we assume that the adversary $\tilde{A}$ has intercepted messages $auth_a = \{h(SID_i), b_a, b_c, T_1, b_d\}$ and $auth_b = \{h(MID_j), c_a, c_b, T_3, c_d\}$. To deceive the unsuspecting receivers, the adversary tries to forge messages $auth_a$ and $auth_b$. However, long-term secrets, such as $\{SID_i, MID_j, GID, \phi\}$, and short-term values, such as $\{r_2, r_3\}$, are unavailable to the adversary $\tilde{A}$. Consequently, MitM and forgery attacks against our protocol flop.

Privileged insider threats are mitigated: In many organisations, some entities have elevated privileges that can be misused to compromise the security of the communication system. This is mostly the case during the registration phase. To curb this threat, we deploy a private *BC* to register the network entities, such as *SU*s and *MS*s. Therefore, critical security tokens, such as $\{a_b, h\,(ID_{TA})\}$, $\{SID_i, GID, G_{pk}, a_e, RC_i\}$ and $\{MID_j, GID, G_{pk}, a_e, RC_j\}$, are forwarded to the *BC* ledger for storage. Given that this ledger is only accessible to properly authenticated entities, network compromise through privileged insiders is prevented.

Physical, session hijacking and side-channelling attacks are prevented: Suppose that the adversary $\tilde{A}$ has physically captured the SU_i. Next, power analysis techniques are deployed to extract stored values $\{h\,(SID_i), h\,(GID), G_{pk}, a_e, RC_i, P\}$. This is followed by an attempt to construct a message $auth_a = \{h(SID_i), b_a, b_c, T_1, b_d\}$, which is forwarded from the SU_i towards the *MS* in an effort to hijack the *SU*'s session. Given that the adversary does not have access to parameters b_a, b_c, T_1 and b_d, these attacks are effectively mitigated.

Replay, desynchronization and DoS attacks are prevented: In our protocol, two messages are exchanged over the public communication channels. These messages include $auth_a = \{h(SID_i), b_a, b_c, T_1, b_d\}$ and $auth_b = \{h(MID_j), c_a, c_b, T_3, c_d\}$. Here, $b_a = h\,(h(SID_i)||h(GID)||G_{pk}||T_1) \oplus a_e$, $b_c = h\,(h(GID)||G_{pk}||T_1||a_e) \oplus r_2.P$, $b_d = h\,(h(GID)||\,r_2.P||a_e) \oplus RC_i$, $c_a = h\,(a_e||r_2.P^*\,||G_{pk}||h(MID_j)||h(GID)||T_3) \oplus b_e$, $c_b = h\,(b_e||G_{pk}||h(MID_j)||T_3) \oplus r_3$ and $c_d = h\,(h(GID)||r_3||b_e) \oplus RC_j$. Evidently, these messages incorporate timestamps $\{T_1, T_3\}$, which are verified at the receiver's end. This effectively curbs any attempts to replay old but valid messages that can overwhelm the network leading to DoS. In addition, these messages incorporate random nonces $\{r_2, r_3\}$ and regional codes, such as RC_j. Therefore, the adversary $\tilde{A}$ cannot easily desynchronize the communication between the *MS* and the SU_i. To address potential drift issues in real-world deployments, the maximum permissible transmission delay ΔT needs to be practically determined for each network. This enables adjustments to be made to ΔT to account for the changing network conditions.

Offline guessing and ephemeral secret key leakage threats are mitigated: In the proposed scheme, the *MS* calculates the session key as $SK_{ms} = h\,(h(SID_i)||h(MID_j)||h(GID)||G_{pk}||b_e||r_2.P^*||T_1||T_3||RC_i^*||RC_j)$, whereas the SU_i computes this session key as $SK_{sm} = h\,(h(SID_i)||h(MID_j)||h(GID)||G_{pk}||b_e^*||r_2.P||T_1||T_3||RC_i^*||RC_j^*)$. Here, $G_{pk} = P.G_{sk}$, $b_e = r_3(r_2.P^*)$, $RC_i^* = h\,(h(GID)||r_2.P^*||a_e^*)\oplus b_d$, $a_e^* = h\,(h(SID_i)||h(GID)||G_{pk}||T_1)\oplus b_a$, $b_a = h\,(h(SID_i)||h(GID)||G_{pk}||T_1) \oplus a_e$, $h\,(h(GID)||r_2.P||a_e) \oplus RC_i$, $a_e = a_d \oplus a_c$, $a_d = h\,(SID_i||GID||G_{pk}||a_c) \oplus G_{pk}$ and $a_c = \phi.P$. These session keys are based on transient secrets $\{r_2, r_3\}$ and long-term secrets $\{SID_i, MID_j, GID, RC_i^*, RC_j, \phi, G_{sk}\}$. For this attack, we consider the following cases.

- Scenario 1: Suppose that the adversary $\tilde{A}$ has access to temporary values $\{r_2, r_3\}$ and attempts to derive session keys SK_{ms} and SK_{sm}. However, without long-term secrets $\{SID_i, MID_j, GID, RC_i^*, RC_j, \phi, G_{sk}\}$, this derivation will flop.
- Scenario 2: Assume that the adversary $\tilde{A}$ has access to long-term secrets $\{SID_i, MID_j, GID, RC_i^*, RC_j, \phi, G_{sk}\}$ and now wants to derive session keys SK_{ms} and SK_{sm}. However, this derivation requires short-term values $\{r_2, r_3\}$. Conversely, r_2 is independently generated at the SU_i, and r_3 is autonomously generated at the *MS*. This presents some difficulties for the adversary $\tilde{A}$ that might attempt to simultaneously and correctly guess these nonces.

Perfect key secrecy: In our protocol, the *MS* derive the session keys as $SK_{ms} = h\,(h(SID_i)||h(MID_j)||h(GID)||G_{pk}||b_e||r_2.P^*||T_1||T_3||RC_i^*||RC_j)$, whereas the SU_i computes its session key as $SK_{sm} = h\,(h(SID_i)||h(MID_j)||h(GID)||G_{pk}||b_e^*||r_2.P||T_1||T_3||RC_i^*||RC_j^*)$. Here, $G_{pk} = P.G_{sk}$, $b_e = r_3(r_2.P^*)$, $RC_i^* = h\,(h(GID)||r_2.P^*||a_e^*) \oplus b_d$, $a_e^* = h\,(h(SID_i)||h(GID)||G_{pk}||T_1)\oplus b_a$, $b_d = h\,(h(GID)||\,r_2.P||a_e)\oplus RC_i$, $b_a = h\,(h(SID_i)||h(GID)||G_{pk}||T_1) \oplus a_e$, $RC_j^* = h\,(h(GID)||r_3^*||b_e^*)\oplus c_d$ and $c_d = h\,(h(GID)||r_3||b_e)\oplus RC_j$. Evidently, these session keys incorporate transient parameters, such as nonces $\{r_2, r_3\}$ and timestamps $\{T_1, T_3\}$. r_2 and T_1 are generated at the SU_i, whereas r_3 and T_3 are generated at the *MS*. Therefore, an attacker with current session keys SK_{ms} and SK_{sm} is unable to use them to derive previous and subsequent session keys. The inability to simultaneously guess temporary values $\{r_2, r_3, T_1, T_3\}$ by the adversary $\tilde{A}$ implies that our protocol upholds perfect session key secrecy.

Conditional privacy and non-repudiation: In our scheme, the *TA* chooses unique identities SID_i, MID_j and *GID* for the SU_i, *MS* and *GWN*, respectively. The *TA* then registers these identities $\{SID_i, MID_j, GID\}$ to the *BC* network. Therefore, the *BC*'s ledger contains history of all gateways, servers and sensors. Therefore, any misbehaving IoMT entity can be easily tracked by the *TA* and eliminated from the network.

Implementation complexity and scalability: In the proposed protocol, the *TA* and *BC* are only involved during the registration process, which happens only once. To reduce implementation complexity and boost scalability, the *TA* and *BC* are never involved in the authentication and session key agreement procedures, which occur frequently. Instead, the SU_i and *MS* mutually authenticate directly without the involvement of any third party, as shown in Fig. 3. As such, the increase in the number of sensors does not adversely increase the implementation complexity. Consequently, network scalability is supported. When patients experience some mobility from their original regional code, their verification is accomplished through the new regional code RC_i^{new}. As such, the proposed scheme effectively supports patient mobility from one region to the other.

5. Performance Evaluation

Most of the authentication protocols in the IoMT have their performance evaluated in terms of supported functionalities, computation, energy and communication overheads. As such, we utilize these performance measures to evaluate our scheme. Thereafter, we compare the obtained values with those obtained in other related protocols.

5.1 Computation Costs

In this subsection, we derive the computation overheads incurred by our scheme during the authentication

and session key setup phase. We designate one-way hashing, ECC point multiplication, PUF, ECC point addition, bilinear pairing, symmetric encryption/decryption, fuzzy extraction and Chebyshev polynomial as T_h, T_{pm}, T_{puf}, T_{pa}, T_b, T_e, T_f and T_C, respectively. The proposed scheme is implemented in a machine with specifications listed in Table 2.

Table 2. Implementation environment

Feature	Description
Hardware	EliteBook 840 G5 Notebook
Processor	Intel Core i5-8350U
Clock frequency	3.6 GHz
RAM	16 GB
Operating system	Ubuntu 24.04.1 LTS
Programming language	Python

In the implementation environment in Table 2, the execution for $T_h \approx 0.012$ ms, $T_{pm} \approx 2.18$ ms, $T_{puf} \approx 0.13$ ms, $T_{pa} \approx 0.625$ ms, $T_b \approx 5.204$ ms, $T_e \approx 0.1403$ ms, $T_f \approx 2.18$ ms and $T_C \approx 1.327$ ms. During the authentication and session key agreement procedures, the SU_i executes $7T_h + T_{pm}$ operations, whereas the MS carries out $7T_h + 2T_{pm}$. As such, the cumulative computation cost of our protocol is $14T_h + 3T_{pm}$. Table 3 presents the computation cost derivation for our scheme, as well as other related protocols.

Table 3. Computation costs

Scheme	Derivation	Total (ms)
Wang et al. [32]	$8T_h + 4T_{pm}$	8.816
Ma et al. [33]	$17T_h + 6T_{pm} + 3T_{pa}$	15.159
Servati and Safkhani [35]	$18T_h + 15T_{pm} + 5T_{pa}$	36.041
Mo et al. [47]	$27T_h + 6T_C$	8.286
Zhang et al. [51]	$2T_h + 3T_{pm} + 2T_b$	16.972
Liu et al. [52]	$38T_h + 6T_{pm}$	13.536
Subramani et al. [57]	$17T_h + 6T_f + 4T_{puf}$	13.804
Proposed	$14T_h + 3T_{pm}$	6.708

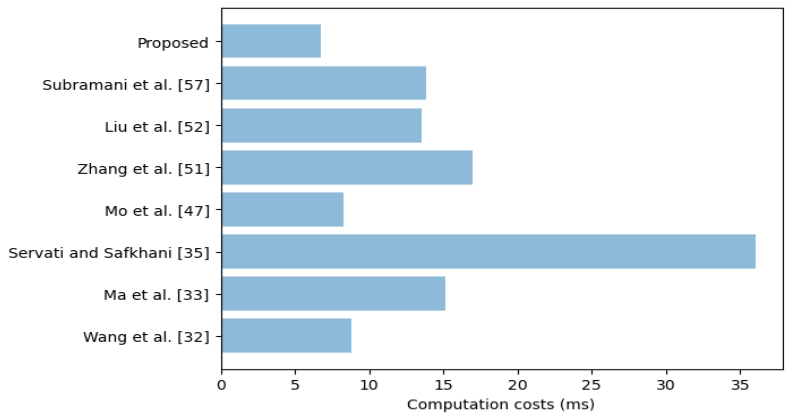

Fig. 5. Comparison of computation costs.

As shown in Fig. 5, the scheme in [35] incurs the longest execution time of 36.041 ms. This is followed by the protocols in [51], [33], [57], [52], [32], and [47] with 16.972, 15.159, 13.804, 13.536, 8.816, and 8.286 ms, respectively.

Moreover, Fig. 4 shows that our proposed scheme incurs the least computation cost of only 6.708 ms. Using the protocol in [47] as the benchmark, this represents a 19.04% reduction in computation overheads.

5.2 Communication Costs

To derive the communication overhead incurred by our scheme, we deploy the sizes of the two messages exchanged between the MS and SU_i during the authentication and session key agreement phase. The messages are $auth_a = \{h(SID_i), b_a, b_c, T_1, b_d\}$ and $auth_b = \{h(MID_j), c_a, c_b, T_3, c_d\}$. Here, we take unique identities, timestamp, pseudo-identities, random nonces and hashing output to be 64, 32, 128, 128 and 160 bits, respectively.

Therefore, $auth_b = \{160 + 160 + 160 + 32 + 160 = 672$ bits$\}$, and $auth_b = \{160 + 160 + 160 + 32 + 160 = 672$ bits$\}$. As such, the cumulative communication overhead for our scheme is 1344 bits or 168 bytes. Table 4 presents the communication costs of our scheme together with the communication overheads of other related schemes.

Table 4. Communication costs

Scheme	Number of messages	Total (bits)
Wang et al. [32]	3	1472
Ma et al. [33]	4	9632
Servati and Safkhani [35]	4	3456
Mo et al. [47]	4	1952
Zhang et al. [51]	2	2816
Liu et al. [52]	4	2858
Subramani et al. [57]	6	3168
Proposed	2	1344

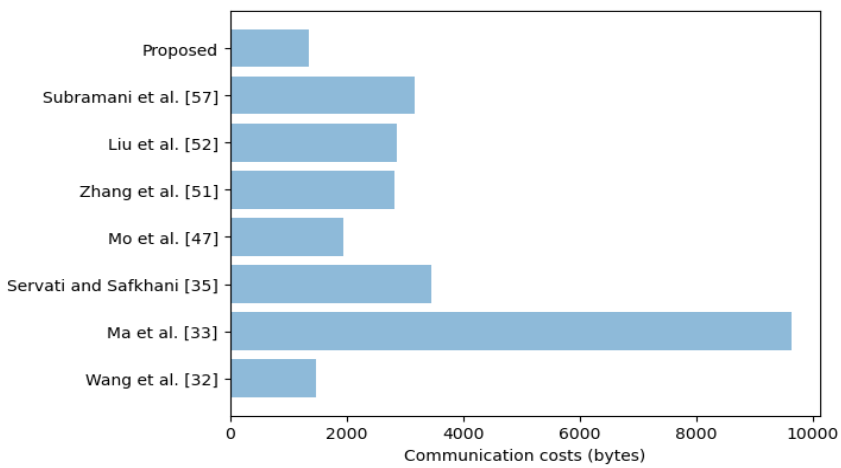

Fig. 6. Comparison of communication costs.

Fig. 6 shows that the protocol in [33] requires the highest communication overhead of 9632 bits. This is followed by the schemes in [35], [57], [52], [51], [47], and [32], with communication costs of 3456, 3168, 2858, 2816, 1952, and 1472 bits, respectively

As shown in Fig. 5, the proposed protocol incurs the least communication overhead of only 1344 bits. Using the communication overhead in [32] as the basis, our scheme results in an 8.7% reduction in communication costs.

5.3 Energy Costs

The energy consumed during the authentication and session key setup is another critical metric for assessing the efficiency of security protocols. Considering the maximum power of the central processing unit as ρ and τ as the cumulative protocol execution time, the energy consumption E is given by $E = \rho \times \tau$. According to [60], $\rho = 10.88$ W; hence, the energy consumption of our protocol is 72.983 mJ. Table 5 presents the energy consumption of our scheme, together with the energy consumption of other related protocols.

Table 5. Energy consumption

Scheme	Energy (mJ)
Wang et al. [32]	95.918
Ma et al. [33]	164.930
Servati and Safkhani [35]	392.126
Mo et al. [47]	90.152
Zhang et al. [51]	184.655
Liu et al. [52]	147.272
Subramani et al. [57]	150.188
Proposed	72.983

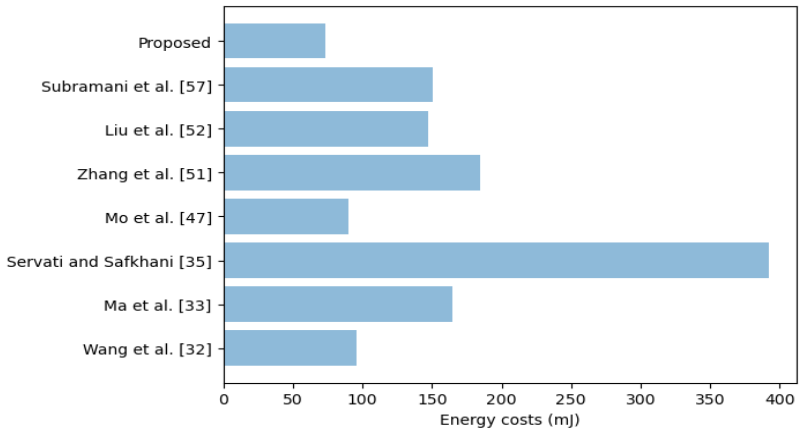

Fig. 7. Comparison of energy costs.

Fig. 7 shows that the protocol developed by [35] requires the highest amount of energy (392.126 mJ) during the authentication and key setup phase. This is followed by the schemes in [51], [33], [57], [52], [32], and [47] with 184.655, 164.930, 150.188, 147.272, 95.918, and 90.152 mJ, respectively. Conversely, the proposed scheme consumes only 72.983 mJ of energy, which is the lowest. Using the scheme in [47] as the benchmark, our scheme results in a 19.04% reduction in energy consumption.

5.4 Supported Functionalities

The proposed scheme offers salient security features that are critical for the protection of messages exchanged between the biosensors and the hospital *MS*s. In addition, it resists numerous attacks that are typical in IoMT environment. We then compare these supported features with the ones supported by other related schemes.

As shown in Table 6, the schemes in [32], [33], [35], [47], [51], [52], [57], and the proposed protocol support 9, 9, 13, 12, 8, 11, 12, and 22 security features, respectively. Therefore, the scheme in [5] is the

most insecure, whereas the proposed scheme is the most secure. Considering the scheme in [51] as the benchmark, our protocol improves the security level by 69.23%. Particularly, the proposed protocol provides conditional privacy and location-aware verification, which the rest of the schemes fail to support. In addition, it mitigates session hijacking and side-channelling, which are ignored in other protocols. Moreover, it prevents against non-repudiation and eavesdropping, which other schemes fail to mitigate, apart from the protocol in [32]. Given that majority of the smart devices in the IoMT are resource-limited, our scheme provides the required levels of security in the most efficient way. It is therefore the most ideal for deployment in this particular environment.

Table 6. Functionalities and security features

	Ma et al. [33]	Wang et al. [32]	Liu et al. [52]	Servati and Safkhani [35]	Subramani et al. [57]	Mo et al. [47]	Zhang et al. [51]	Proposed
Security functionalities								
Authentication	√	√	√	√	√	√	√	√
Session key agreement	√	√	√	√	√	√	×	√
Perfect key secrecy	√	×	√	√	√	√	×	√
Untraceability	√	×	√	×	√	×	√	√
Anonymity	√	×	√	√	√	√	√	√
Formal verification	√	×	√	√	√	√	√	√
Location-aware verification	×	×	×	×	×	×	×	√
Conditional privacy	×	×	×	×	×	×	×	√
Non-repudiation	×	√	×	×	×	×	×	√
Robust against:								
ESL	√	×	×	√	√	×	×	√
Eavesdropping	×	√	×	×	×	×	×	√
Impersonation	√	√	√	√	×	√	√	√
MitM	×	√	√	√	×	√	×	√
Forgery	×	√	×	×	√	×	√	√
Privileged insider	×	×	×	√	×	√	×	√
Physical threats	√	×	√	√	√	√	√	√
Session hijacking	×	×	×	×	×	×	×	√
Side-channelling	×	×	×	×	×	×	×	√
Replays	×	√	√	√	√	√	√	√
Desynchronization	×	×	×	×	√	√	×	√
DoS	×	√	×	√	√	√	×	√
Offline guessing	×	×	√	√	×	×	×	√

√ = supported; × = missing or not considered.

5.5 BC Implementation

In this section, we use Hyperledger Fabric to implement the *BC*-based registration. Here, the *TA* creates block Blk_j based on transactions $\{BC_a, R_b\}$. As such, Blk_j comprises numerous transactions encrypted using the *TA*'s public key a_c. Using the Elliptic Curve Digital Signature Algorithm, the signature on Blk_j is generated by the *TA*. The structure of Blk_j is shown in Fig. 8, whose header is composed of the block version (V_B), previous block hash (H_{pb}), Merkel tree root (R_{Mt}), timestamp (S_t), block creator (ID_{TA}) and signer's public key (a_c). Conversely, the block payload consists of encrypted transactions $\{E_{a_c}(BC_a, R_b)\}$,

current block hash (H_{cb}) and signature on H_{cb} (H_{sig}). Basically, $H_{sig} = ECDSA.Sig_{\phi}(H_{cb})$, where is the private key belonging to the *TA*.

Header	
Block version	V_B
Previous blockchain	H_{pb}
Merkel tree root	R_{Mt}
Timestamp	S_t
Block creator	ID_{TA}
Public key of singer	a_c
Payload	
List of enciphered transactions	$\{E_{a_c}(BC_a, R_b)\}$
Current block hash	H_{cb}
Signature on H_{cb}	H_{sig}

Fig. 8. Blk_j structure.

1. T_L generates current timestamp T_c for each T_F
2. Derive $\rho = E_{a_c}(R_{vt}, T_c)$
3. Forward $m_a = \{Blk_j, \rho\}$ to all T_{F_k}, (k = 1, 2, …$\forall_k \neq T_L$)
4. **For** each T_{F_k} **do**:
5. Receiving m_a from T_L at timestamp T_c^*
6. Calculate (R_{vt}^*, T_c) = $D_{\phi}(\rho)$
7. **If** {T_c, R_{Mt}, H_{cb}, H_{sig} } are valid **then**:
8. Derive $\gamma = E_{a_c}(R_{vt}^*, R_{vr}, S_{vs})$
9. Forward γ to T_L
10. **End if**
11. **End for**
12. Set $C_v \leftarrow 0$
13. **For** each received γ from T_F **do**:
14. Calculate (R_{vt}^*, R_{vr}, S_{vs}) = $D_{\phi}(\gamma)$
15. **If** {$R_{vt}^* = R_{vt}$} and {R_{vr} , S_{vs}}are legitimate **then**:
16. $C_v = C_v + 1$
17. **End if**
18. **End for**
19. **If** $C_v > 2(N_f)$ **then**:
20. **Forward** R_c to all T_F
21. Upload Blk_j to BC
22. **End if**

Fig. 9. Block validation and uploading to the *BC*.

To validate and add blocks in the *BC*, we deploy the practical Byzantine fault tolerance (PBFT) due to its resilience to Byzantine faults and its ability to build a consensus in the face of malicious nodes or unexpected failure of some nodes. This process starts by deploying the leader selection algorithm to choose a leader T_L in the peer-to-peer network of q *TA*s. Afterwards, Blk_j is forwarded to T_L for consensus building, which will facilitate the validation and uploading of Blk_j to the *BC*. The pseudocode for the block validation and uploading to the *BC* is shown in Fig. 9. Here, we denote *BC*, follower *TA*, voting request, voting response, Blk_j verification status, vote counter, number of faulty *TA* nodes and commit response as *BC*, T_F, R_{vt}, R_{vr}, S_{vs}, C_v, N_f and R_c, respectively. We then evaluate the latency, storage and energy costs associated with the *BC*-based registration process.

Energy usage is a crucial performance measure for *BC* networks. As such, we investigate the effect of the number of mined blocks on energy usage, as shown in Fig. 10. Based on the obtained output, energy

consumption linearly increases with the number of mined blocks. In *BC* networks, energy is consumed during block verification and addition to the chain.

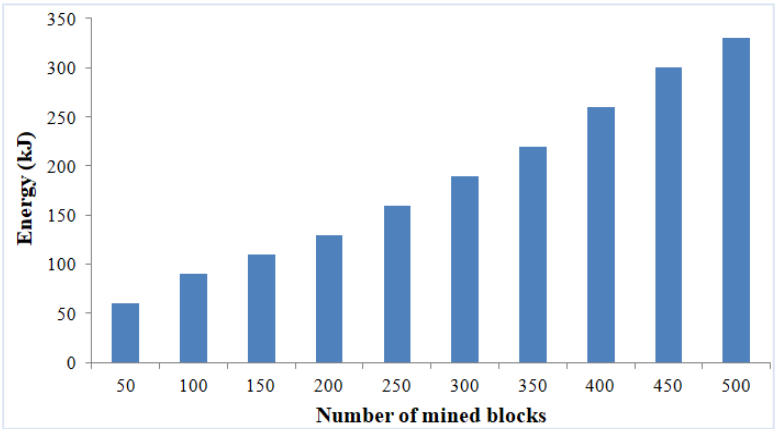

Fig. 10. Energy usage.

As such, the higher the number of mined blocks, the higher the energy required to validate and add blocks to the chain. To determine latency, we measure the difference between block submission and confirmation time. Therefore, this latency also includes propagation time, as well as time taken to build a consensus. We also measure the minimum, maximum and average latency against the number of nodes and blocks.

The obtained results are presented in Fig. 11. Evidently, the number of nodes increases with the measured latency. The reason is that transactions or blocks have to take a long propagation time to reach all the network nodes. In addition, consensus building takes a long time as the number of nodes increases.

To investigate the effect of the number of nodes on storage overheads, we increment the number of nodes in steps of 10 up from the initial value of 10 to a maximum of 100, as shown in Fig. 12. The results show that the number of nodes increases with the storage overheads.

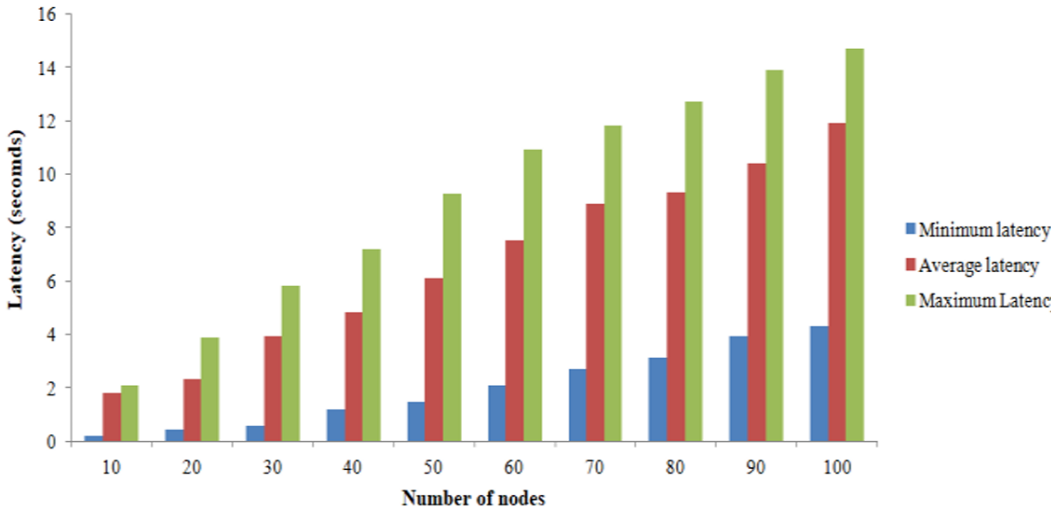

Fig. 11. Latency for varying number of nodes.

This is justified by the replication of data across all nodes, where each network node is required to store an entire copy of the *BC*. This is significant because it helps mitigate single point of failure, preserve fault

tolerance and achieve high availability. The replicated copy on each node also helps these nodes to independently validate the transactions in blocks.

This verification enables the nodes to participate in consensus mechanisms, such as PBFT. Therefore, a high number of nodes within the *BC* network implies increased levels of data replication. This effectively translates to higher storage requirements to store the replicated *BC* data.

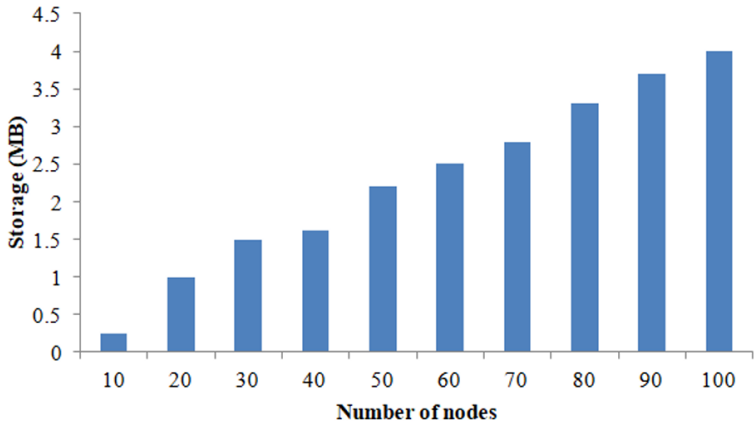

Fig. 12. Storage overheads variations.

6. Conclusion

The IoMT has contributed to the enhanced quality of healthcare, patient experience, decongestion of hospitals and reductions in healthcare costs. However, security and privacy challenges are serious issues that can have catastrophic repercussions in this environment. Any successful network infiltration by malicious entities can lead to leakage of patient sensitive data, modification of transmitted data and DoS. All these attacker capabilities can lead to serious outcomes, including loss of patient life due to delayed or wrong medical interventions. Although many security schemes have been developed recently, these approaches often have security vulnerabilities or are inefficient for the small, resource-constrained biosensors. In this paper, an efficient authentication scheme is developed. It is shown to resist numerous cyber threats such as eavesdropping, session hijacking, impersonation and desynchronization. Its execution, energy and communication overheads are the lowest amongst its peers. Therefore, the proposed scheme is not only robust but also the most efficient, making it ideal for implementation in resource-limited IoMT biosensors. In our scheme, we deploy timestamps to mitigate replay threats. However, if the maximum transmission delay is large enough, adversaries can have enough time to modify and forward the intercepted messages. Future work lies in the practical estimation of this maximum transmission latency to ensure that it is optimal. In addition, the proposed scheme needs to be implemented on an actual IoMT environment to assess its performance in resource-constrained devices, and its sensor constraints need to be emulated in platforms like Raspberry Pi or Arduino to strengthen its practicality.

Author's Contributions

Conceptualization, ZAA, VON, MAH, JM, MAA, ZAH, AJYA, AHA, AAA, HAN; Investigation, ZAA, VON, MAH, JM, MAA; Methodology, ZAA, VON, MAH, JM, MAA; Supervision, ZAA, JM; Writing of the original draft, ZAA, VON, MAH, JM, MAA; Writing of the review and editing, ZAH, AJYA, AHA, AAA, HAN; Software, ZAH, AJYA, AHA, AAA, HAN; Validation, ZAA, VON, MAH, JM, MAA; Data curation, ZAA, VON, MAH, JM, MAA; Visualization, ZAH, AJYA, AHA, AAA, HAN. Formal analysis, ZAA, VON, MAH, JM, MAA; Resources, ZAH, AJYA, AHA, AAA, HAN.

Funding

This research was financially supported by the Open Research Fund from Guangdong Laboratory of Artificial Intelligence and Digital Economy (SZ), under Grant No.GML-KF-24-04.

Competing Interests

The authors declare that they have no competing interests.

References

[1] I. Al Khatib, A. Shamayleh, and M. Ndiaye, "Healthcare and the internet of medical things: applications, trends, key challenges, and proposed resolutions," *Informatics*, vol. 11, no. 3, article no. 47, 2024. https://doi.org/10.3390/informatics11030047

[2] Z. Ashfaq, A. Rafay, R. Mumtaz, S. M. H. Zaidi, H. Saleem, S. A. R. Zaidi, S. Mumtaz, and A. Haque, "A review of enabling technologies for Internet of Medical Things (IoMT) Ecosystem," *Ain Shams Engineering Journal*, vol. 13, no. 4, article no. 101660, 2022. https://doi.org/10.1016/j.asej.2021.101660

[3] J. Pourbemany, Y. Zhu, and R. Bettati, "A survey of wearable devices pairing based on biometric signals," *IEEE Access*, vol. 11, pp. 26070-26085, 2023. https://doi.org/10.1109/ACCESS.2023.3254499

[4] D. T. Phan, C. H. Nguyen, T. D. P. Nguyen, L. H. Tran, S. Park, J. Choi, B. Lee, and J. Oh, "A flexible, wearable, and wireless biosensor patch with internet of medical things applications," *Biosensors*, vol. 12, no. 3, article no. 139, 2022. https://doi.org/10.3390/bios12030139

[5] M. El Khatib, H. M. Alzoubi, S. Hamidi, M. Alshurideh, A. Baydoun, and A. Al-Nakeeb, "Impact of using the internet of medical things on e-healthcare performance: blockchain assist in improving smart contract," *Clinico-Economics and Outcomes Research*, vol. 15, pp. 397-411, 2023. https://doi.org/10.2147/CEOR.S407778

[6] V. O. Nyangaresi, Z. A. Abduljabbar, K. A. A. Mutlaq, M. A. Hussain, and Z. A. Hussien, "Forward and backward key secrecy preservation scheme for medical Internet of things," in *Human-Centric Smart Computing*. Singapore: Springer, 2022, pp. 15-29. https://doi.org/10.1007/978-981-19-5403-0_2

[7] T. E. Ali, F. I. Ali, P. Dakic, and A. D. Zoltan, "Trends, prospects, challenges, and security in the healthcare internet of things," *Computing*, vol. 107, no. 1, article no. 28, 2025. https://doi.org/10.1007/s00607-024-01352-4

[8] S. E. El-deep, A. A. Abohany, K. M. Sallam, and A. A. A. El-Mageed, "A comprehensive survey on impact of applying various technologies on the internet of medical things," *Artificial Intelligence Review*, vol. 58, no. 3, article no. 86, 2025. https://doi.org/10.1007/s10462-024-11063-z

[9] S. Shreya, K. Chatterjee, and A. Singh, "A smart secure healthcare monitoring system with Internet of Medical Things," *Computers and Electrical Engineering*, vol. 101, article no. 107969, 2022. https://doi.org/10.1016/j.compeleceng.2022.107969

[10] P. Mishra and G. Singh, "Internet of medical things healthcare for sustainable smart cities: current status and future prospects," *Applied Sciences*, vol. 13, no. 15, article no. 8869, 2023. https://doi.org/10.3390/app13158869

[11] B. Bhushan, A. Kumar, A. K. Agarwal, A. Kumar, P. Bhattacharya, and A. Kumar, "Towards a secure and sustainable internet of medical things (IoMT): requirements, design challenges, security techniques, and future trends," *Sustainability*, vol. 15, no. 7, article no. 6177, 2023. https://doi.org/10.3390/su15076177

[12] M. Jawad, A. A. Yassin, H. A. A. AL-Asadi, Z. A. Abduljabbar, and V. O. Nyangaresi, "Towards building multi-factor authentication scheme for users in the healthcare sector based on blockchain technology," in *Computer Science On-line Conference*. Cham, Switzerland: Springer, 2024, pp. 694-713. https://doi.org/10.1007/978-3-031-70300-3_52

[13] F. I. Ali, T. E. Ali, and A. H. Hamad, "Telemedicine framework in COVID-19 pandemic," in *Proceedings of 2022 International Conference on Engineering and Emerging Technologies (ICEET)*, Kuala Lumpur, Malaysia, 2022, pp. 1-8. https://doi.org/10.1109/ICEET56468.2022.10007389

[14] S. S. Chopade, H. P. Gupta, and T. Dutta, "Survey on sensors and smart devices for IoT enabled intelligent healthcare system," *Wireless Personal Communications*, vol. 131, no. 3, pp. 1957-1995, 2023. https://doi.org/10.1007/s11277-023-10528-8

[15] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent advances in the internet-of-medical-things (IoMT) systems security," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8707-8718, 2021. https://doi.org/10.1109/JIOT.2020.3045653

[16] S. F. Ahmed, M. S. B. Alam, S. Afrin, S. J. Rafa, N. Rafa, and A. H. Gandomi, "Insights into Internet of Medical Things (IoMT): data fusion, security issues and potential solutions," *Information Fusion*, vol. 102, article no. 102060, 2024. https://doi.org/10.1016/j.inffus.2023.102060

[17] S. Dong, H. Su, Y. Xia, F. Zhu, X. Hu, and B. Wang, "A comprehensive survey on authentication and attack detection schemes that threaten it in vehicular ad-hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 12, pp. 13573-13602, 2023. https://doi.org/10.1109/TITS.2023.3297527

[18] V. O. Nyangaresi, Z. A. Abduljabbar, J. Ma, and M. A. Al Sibahee, "Verifiable security and privacy provisioning protocol for high reliability in smart healthcare communication environment," in *Proceedings of 2022 4th Global Power, Energy and Communication Conference (GPECOM)*, Nevsehir, Turkey, 2022, pp. 569-574. https://doi.org/10.1109/GPECOM55404.2022.9815685

[19] M. Asif, M. Abrar, A. Salam, F. Amin, F. Ullah, S. Shah, and H. AlSalman, "Intelligent two-phase dual authentication framework for Internet of Medical Things," *Scientific Reports*, vol. 15, no. 1, article no. 1760, 2025. https://doi.org/10.1038/s41598-024-84713-5

[20] S. Kumar, D. Kumar, H. Lamkuche, V. S. Sharma, H. K. Alkahtani, M. Elsadig, and M. A. Bivi, "SHC: 8-bit compact and efficient S-box structure for lightweight cryptography," *IEEE Access*, vol. 12, pp. 39430-39449, 2024. https://doi.org/10.1109/ACCESS.2024.3372388

[21] S. Dong, K. Abbas, M. Li, and J. Kamruzzaman, "Blockchain technology and application: an overview," *PeerJ Computer Science*, vol. 9, article no. e1705, 2023. https://doi.org/10.7717/peerj-cs.1705

[22] A. Salam, M. Abrar, F. Ullah, I. A. Khan, F. Amin, and G. S. Choi, "Efficient data collaboration using multi-party privacy preserving machine learning framework," *IEEE Access*, vol. 11, pp. 138151-138164, 2023. https://doi.org/10.1109/ACCESS.2023.3339750

[23] M. M. Islam and M. Shamshuzzoha, "Securing wireless body area networks data transmission with machine learning: a cross-tier framework for anomaly detection and intrusion prevention," *Computational and Structural Biotechnology Reports*, vol. 2, article no. 100031, 2025. https://doi.org/10.1016/j.csbr.2025.100031

[24] J. Herbst, M. Rub, S. P. Sanon, C. Lipps, and H. D. Schotten, "Medical data in wireless body area networks: device authentication techniques and threat mitigation strategies based on a Token-Based communication approach," *Network*, vol. 4, no. 2, pp. 133-149, 2024. https://doi.org/10.3390/network4020007

[25] D. Jiang, G. Zhang, O. W. Samuel, F. Liu, and H. Xiao, "Dual-factor WBAN enhanced authentication system based on iris and ECG descriptors," *IEEE Sensors Journal*, vol. 22, no. 19, pp. 19000-19009, 2022. https://doi.org/10.1109/JSEN.2022.3198645

[26] M. Serrano, A. Gyrard, M. Boniface, P. Grace, N. Georgantas, R. Agarwal, et al., "Cross-domain interoperability using federated interoperable semantic IoT/Cloud testbeds and applications: the FIESTA-IoT approach," in *Building the Future Internet Through FIRE*. Gistrup, Denmark: River Publishers, 2022, pp. 287-321. https://doi.org/10.1201/9781003337447-12

[27] Z. U. Rehman, S. Altaf, S. Ahmad, S. Huda, A. M. Al-Shayea, and S. Iqbal, "An efficient, hybrid authentication using ECG and lightweight cryptographic scheme for WBAN," *IEEE Access*, vol. 9, pp. 133809-133819, 2021. https://doi.org/10.1109/ACCESS.2021.3115706

[28] J. Srinivas, A. K. Das, M. Wazid, and N. Kumar, "Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial Internet of Things," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 6, pp. 1133-1146, 2020. https://doi.org/10.1109/TDSC.2018.2857811

[29] Y. Guo and Y. Guo, "CS-LAKA: a lightweight authenticated key agreement protocol with critical security properties for IoT environments," *IEEE Transactions on Services Computing*, vol. 16, no. 6, pp. 4102-4114, 2023. https://doi.org/10.1109/TSC.2023.3309860

[30] Z. A. Ali, Z. A. Abduljabbar, H. A. A. Al-Asadi, V. O. Nyangaresi, I. Q. Abduljaleel, and A. Aldarwish, "A provably secure anonymous authentication protocol for consumer and service provider information transmissions in smart grids," *Cryptography*, vol. 8, no. 2, article no. 20, 2024. https://doi.org/10.3390/cryptography8020020

[31] I. Nagasundharamoorthi, P. Venkatesan, and P. Velusamy, "Hash message authentication codes for securing data in wireless body area networks," *Concurrency and Computation: Practice and Experience*, vol. 36, no. 5, article no. e7934, 2024. https://doi.org/10.1002/cpe.7934

[32] K. Wang, Y. Hong, Y. Li, R. Yan, and J. Feng, "A distributed zero-trust scheme for airborne wireless sensor networks using dynamic identity authentication," *Scientific Reports*, vol. 15, no. 1, article no. 8036, 2025. https://doi.org/10.1038/s41598-025-91957-2

[33] Y. Ma, Y. Ma, J. Zhang, and Q. Cheng, "An improved anonymous authentication protocol in wireless body area networks," *IEEE Internet of Things Journal*, vol. 12, no. 9, pp. 12885-12895, 2025. https://doi.org/10.1109/JIOT.2024.3523111

[34] K. Sowjanya, M. Dasgupta, and S. Ray, "An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems," *International Journal of Information Security*, vol. 19, no. 1, pp. 129-146, 2020. https://doi.org/10.1007/s10207-019-00464-9

[35] M. R. Servati and M. Safkhani, "ECCbAS: an ECC based authentication scheme for healthcare IoT systems," *Pervasive and Mobile Computing*, vol. 90, article no. 101753, 2023. https://doi.org/10.1016/j.pmcj.2023.101753

[36] A. Salehi Shahraki, H. Lauer, M. Grobler, A. Sakzad, and C. Rudolph, "Access control, key management, and trust for emerging wireless body area networks," *Sensors*, vol. 23, no. 24, article no. 9856, 2023. https://doi.org/10.3390/s23249856

[37] K. A. A. Mutlaq, V. O. Nyangaresi, M. A. Omar, Z. A. Abduljabbar, I. Q. Abduljaleel, J. Ma, and M. A. Al Sibahee, "Low complexity smart grid security protocol based on elliptic curve cryptography, biometrics and hamming distance," *PLOS One*, vol. 19, no. 1, article no. e0296781, 2024. https://doi.org/10.1371/journal.pone.0296781

[38] M. Nikooghadam and H. Amintoosi, "A secure and robust elliptic curve cryptography-based mutual authentication scheme for session initiation protocol," *Security and Privacy*, vol. 3, no. 1, article no. e92, 2020. https://doi.org/10.1002/spy2.92

[39] M. Kumar and S. Chand, "A lightweight cloud-assisted identity-based anonymous authentication and key agreement protocol for secure wireless body area network," *IEEE Systems Journal*, vol. 15, no. 2, pp. 2779-2786, 2021. https://doi.org/10.1109/JSYST.2020.2990749

[40] F. Li, Y. Han, and C. Jin, "Cost-effective and anonymous access control for wireless body area networks," *IEEE Systems Journal*, vol. 12, no. 1, pp. 747-758, 2018. https://doi.org/10.1109/JSYST.2016.2557850

[41] S. Banerjee, V. Odelu, A. K. Das, J. Srinivas, N. Kumar, S. Chattopadhyay, and K. K. R. Choo, "A provably secure and lightweight anonymous user authenticated session key exchange scheme for Internet of Things deployment," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8739-8752, 2019. https://doi.org/10.1109/JIOT.2019.2923373

[42] S. Liu, D. Xie, Z. Li, F. Chen, W. Bian, and T. Wang, "Many-to-one lightweight batch authentication key agreement for wireless body area networks," *IEEE Internet of Things Journal*, vol. 12, no. 6, pp. 7225-7239, 2025. https://doi.org/10.1109/JIOT.2024.3493419

[43] I. Ullah, A. Alomari, N. Ul Amin, M. A. Khan, and H. Khattak, "An energy efficient and formally secured certificate-based signcryption for wireless body area networks with the internet of things," *Electronics*, vol. 8, no. 10, article no. 1171, 2019. https://doi.org/10.3390/electronics8101171

[44] Y. Xie, S. Zhang, X. Li, Y. Li, and Y. Chai, "CasCP: efficient and secure certificateless authentication scheme for wireless body area networks with conditional privacy-preserving," *Security and Communication Networks*, vol. 2019, article no. 5860286, 2019. https://doi.org/10.1155/2019/5860286

[45] Y. Liao, Y. Liu, Y. Liang, Y. Wu, and X. Nie, "Revisit of certificateless signature scheme used to remote authentication schemes for wireless body area networks," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 2160-2168, 2020. https://doi.org/10.1109/JIOT.2019.2959602

[46] C. Li and C. Xu, "Efficient anonymous authentication for wireless body area networks," *IEEE Access*, vol. 10, pp. 80015-80026, 2022. https://doi.org/10.1109/ACCESS.2022.3180165

[47] J. Mo, Z. Zhang, and Y. Lin, "A practically secure two-factor and mutual authentication protocol for distributed wireless sensor networks using PUF," *Electronics*, vol. 14, no. 1, article no. 10, 2024. https://doi.org/10.3390/electronics14010010

[48] C. Peng, M. Luo, L. Li, K. K. R. Choo, and D. He, "Efficient certificateless online/offline signature scheme for wireless body area networks," *IEEE Internet of Things Journal*, vol. 8, no. 18, pp. 14287-14298, 2021. https://doi.org/10.1109/JIOT.2021.3068364

[49] P. Prameela, "Enhanced certificateless security improved anonymous access control with obfuscated quality-aware confidential data discovery and dissemination protocol in WBAN," *International Journal of*

Pure and Applied Mathematics, vol. 118, no. 18, pp. 2627-2635, 2018. https://acadpubl.eu/jsi/2018-118-18/articles/18c/40.pdf

[50] M. A. Al Sibahee, V. O. Nyangaresi, Z. A. Abduljabbar, C. Luo, J. Zhang, and J. Ma, "Two-factor privacy-preserving protocol for efficient authentication in Internet of Vehicles networks," *IEEE Internet of Things Journal*, vol. 11, no. 8, pp. 14253-14266, 2024. https://doi.org/10.1109/JIOT.2023.3340259

[51] J. Zhang, Q. Zhang, Z. Li, X. Lu, and Y. Gan, "A lightweight and secure anonymous user authentication protocol for wireless body area networks," *Security and Communication Networks*, vol. 2021, article no. 4939589, 2021. https://doi.org/10.1155/2021/4939589

[52] S. Liu, Z. Wang, and C. M. Chen, "A blockchain-assisted drug management and authentication scheme in IoMT," *IEEE Internet of Things Journal*, vol. 12, no. 16, pp. 34283-34296, 2025. https://doi.org/10.1109/JIOT.2025.3577701

[53] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K. K. R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Computer Networks*, vol. 129(Part 2), pp. 429-443, 2017. https://doi.org/10.1016/j.comnet.2017.03.013

[54] M. Masud, G. S. Gaba, K. Choudhary, M. S. Hossain, M. F. Alhamid, and G. Muhammad, "Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2649-2656, 2022. https://doi.org/10.1109/JIOT.2021.3080461

[55] M. Zia, M. S. Obaidat, K. Mahmood, S. Shamshad, M. A. Saleem, and S. A. Chaudhry, "A provably secure lightweight key agreement protocol for wireless body area networks in healthcare system," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1683-1690, 2023. https://doi.org/10.1109/TII.2022.3202968

[56] S. Shihab and R. AlTawy, "Lightweight authentication scheme for healthcare with robustness to desynchronization attacks," *IEEE Internet of Things Journal*, vol. 10, no. 20, pp. 18140-18153, 2023. https://doi.org/10.1109/JIOT.2023.3279035

[57] J. Subramani, A. Maria, A. S. Rajasekaran, and F. Al-Turjman, "Lightweight privacy and confidentiality preserving anonymous authentication scheme for WBANs," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3484-3491, 2022. https://doi.org/10.1109/TII.2021.3097759

[58] Y. Xia, R. Qi, S. Ji, J. Shen, T. Miao, and H. Wang, "PUF-assisted lightweight group authentication and key agreement protocol in smart home," *Wireless Communications and Mobile Computing*, vol. 2022, article no. 8865158, 2022. https://doi.org/10.1155/2022/8865158

[59] Y. Ming, P. Yang, H. Mahdikhani, and R. Lu, "A secure one-to-many authentication and key agreement scheme for industrial IoT," *IEEE Systems Journal*, vol. 17, no. 2, pp. 2225-2236, 2023. https://doi.org/10.1109/JSYST.2022.3209868

[60] B. D. Deebak and S. O. Hwang, "A cloud-assisted medical cyber-physical system using a privacy-preserving key agreement framework and a Chebyshev chaotic map," *IEEE Systems Journal*, vol. 17, no. 4, pp. 5543-5554, 2023. https://doi.org/10.1109/JSYST.2023.3303460