sensors

Article

Blockchain Enabled Anonymous Privacy-Preserving Authentication Scheme for Internet of Health Things

Arun Sekar Rajasekaran [1], Azees Maria [2], Maheswar Rajagopal [3] and Josip Lorincz [4,*]

[1] Department of ECE, KPR Institute of Engineering and Technology, Coimbatore 641407, India
[2] School of Computer Science and Engineering, VIT-AP University, Inavolu, Beside AP Secretariat, Amaravathi 522237, India
[3] Department of ECE, Centre for IoT and AI (CITI), KPR Institute of Engineering and Technology, Coimbatore 641407, India
[4] Faculty of Electrical Engineering, Mechanical Engineering and Naval Architecture (FESB), University of Split, 21000 Split, Croatia
* Correspondence: josip.lorincz@fesb.hr

Abstract: The Internet of Health Things (IoHT) has emerged as an attractive networking paradigm in wireless communications, integrated devices and embedded system technologies. In the IoHT, real-time health data are collected through smart healthcare sensors and, in recent years, the IoHT has started to have an important role in the Internet of Things technology. Although the IoHT provides comfort in health monitoring, it also imposes security challenges in maintaining patient data confidentiality and privacy. To overcome such security issues, in this paper, a novel blockchain-based privacy-preserving authentication scheme is proposed as an approach for achieving efficient authentication of the patient without the involvement of a trusted entity. Moreover, a secure handover authentication mechanism that ensures avoiding the patient re-authentication in multi-doctor communication scenarios and revoking the possible malicious misbehavior of medical professionals in the IoHT communication with the patient is developed. The performance of the proposed authentication and handover scheme is analyzed concerning the existing state-of-the-art authentication schemes. The results of the performance analyses reveal that the proposed authentication scheme is resistant to different types of security attacks. Moreover, the results of analyses show that the proposed authentication scheme outperforms similar state-of-the-art authentication schemes in terms of having lower computational, communication and storage costs. Therefore, the novel authentication and handover scheme has proven practical applicability and represents a valuable contribution to improving the security of communication in IoHT networks.

Keywords: wireless; IoT; health; private key; attack; secure; privacy; sensor; network; cryptography

check for updates

Citation: Rajasekaran, A.S.; Maria, A.; Rajagopal, M.; Lorincz, J. Blockchain Enabled Anonymous Privacy-Preserving Authentication Scheme for Internet of Health Things. *Sensors* **2023**, *23*, 240. https://doi.org/10.3390/s23010240

Academic Editor: Guanding Yu

Received: 24 November 2022
Revised: 13 December 2022
Accepted: 20 December 2022
Published: 26 December 2022

1. Introduction

Due to the growing and aging of the general population, healthcare has been confronted with a number of new issues. The Internet of Health Things (IoHT) is a key component in the Internet of Things (IoT) healthcare applications, where wireless transmission of sensing signals over air serves as a channel for data transmission between entities (patients and medical staff). The IoHT is an innovative solution that can serve the demands of both local and remote medical applications. In today's context, the IoHT uses sophisticated sensors and wearable devices in combination with cloud computing, IoT and wireless networking to gather real-time biological data from the patient's body. The IoHT, as part of a smart healthcare system [1,2], can provide excellent medical monitoring options for different categories of patients, particularly the elderly. The IoHT has been developed for healthcare systems using advanced information and communication technology. The IoHT offers a variety of monitoring services in the healthcare industry, allowing doctors to have a closer status of specific medical parameters of their patients [3–7]. The implementation of the IoHT technology is low-cost and uses non-invasive medical devices. Moreover, the IoHT is an important component of mobile health monitoring systems and dramatically improves healthcare quality and efficiency.

In monitoring the health conditions of elderly people or general people with some health problems remotely, the IoHT starts to play an important role. For example, in the IoHT networks, sensor nodes collect health information such as the patient's pulse, heart rate, blood sugar and other symptoms of possible sickness. For the purpose of monitoring, diagnosis or treatment, such information is transferred to remote servers that are accessible to healthcare specialists via communication technology. Since the first introduction of the IoHT as a concept, there has been a major focus on increasing the security of data transfer, while reducing the IoHT communication and computation costs. Sensing devices in the IoHT transmit information about the human body at any time and from any location. Therefore, the reliable sending of sensing information of the individual is of vital importance.

For monitoring health-related data from a remote distance, the information collected from the sensors should be transferred securely by means of a wireless medium. However, in the real-life implementation of the IoHT technology, the confidential data of the patients can be hacked by intruders and this imposes a serious security problem. To overcome such security challenges, in this paper a novel authentication scheme is proposed as an approach for achieving efficient authentication of the patient without the involvement of a trusted entity.

The IoHT network is generally made up of four parts: the transmitter, the receiver, the battery and the central processing server. Physiological sensors, environmental sensors and biokinetic sensors are types of sensors that are used to monitor real-time data related to human health and well-being. The main goal of the IoHT is to simplify and increase the speed, precision and reliability of sensor/actuator communication within, on or near a human body. The IoHT has the capability to communicate with the Internet as well as other wireless technologies such as ZigBee, wireless sensor networks (WSNs), Bluetooth, video surveillance and mobile cellular networks. There are two different types of sensors used in practical IoHT applications. The first is *in-body communication sensors* where the sensors or nodes for establishing IoHT communication are positioned inside the human body. The medical implant communication system is used for this purpose. The second application of sensors is *on-body communication sensors,* where interaction between wearable devices and the body occurs mostly through sensory components that are implanted in the human body [8–10].

The IoHT must include several required key features such as *trustability,* low *transmission latency, security, confidentiality, integrity and availability*. *Trustability* means that medical data of high precision is included in the data transmission chain by IoHT wearable devices or sensors, and the source of this data must be trustable. *Transmission latency* takes into account that some medical applications that deal with emergency data are not designed to sustain long response times. As a result, assured minimal transmission latency or real-time transmission is required. *Security* is related to the fact that the system should be capable of handling personal and sensitive data and data security and secrecy must be ensured. *Confidentiality* assumes that only authorized persons can have access to the data, and they must be validated by some authentication process before accessing it. Furthermore, data secrecy must be guaranteed in any phase of data processing, i.e., during the data transmission and storage phase. *Integrity* ensures that no unauthorized party should be allowed to alter sensing data or central processing device configurations. Furthermore, the data's source should be reliable. *Availability* means that the information and sensing devices must always be available to authorized organizations and an unauthorized person(s) must not be able to interrupt communication or create a negative impact on the equipment.

The IoHT technology is used in both medical and non-medical applications that support health monitoring. Medical applications are characterized by health monitoring devices that are dedicated to monitoring human medical parameters (heart rate, blood pressure, electrocardiogram (ECG), etc.). Examples of non-medical applications include navigation, time, distance, direction, surrounding temperature, etc., and that information may all be monitored using non-medical sensor devices such as sports sensors. Monitored information is through a concept known as telehealth care used to deliver healthcare over long distances by means of information and communication technology (ICT). Therefore, the IoHT as a technology is legal, affordable and easy to use.

There are several advantages of wireless IoT networks over wired networks, including the elimination of lengthy wired communication lines and the threat of the entire system collapsing if parts of the network or specific node fails. Despite the various advantages of wireless IoT networks, the IoHT has some disadvantages such as limited storage capacity, susceptibility to the impact of noise or interference and continuous power supply issues.

However, cloud computing arose as a solution to the IoHT technology's limited storage capacity. Several networking concepts are commonly employed in the healthcare industry to deliver real-time patient monitoring and services. Although the medical expert may access a patient's cloud-based data from any location on the planet, the patient's sensitive data are transmitted over insecure cloud-based networks. Since only legitimate users have access to their data and services, there is a need for a strong user authentication system. Due to the fact that the physiological parameters of patients are extremely sensitive in terms of privacy, secure communication in the IoHT networks is of great importance. Additionally, security risks arise as a result of the open nature of cloud computing and wireless connectivity. Secure user authentication is thus required because the patient's data is sent over insecure Internet networks [11,12]. Therefore, data security methods are established using some components such as transmission over trusted gateway devices or other highly reliable components and through introducing different authentication schemes for securing the IoHT data transmission. The trusted device may be a smartphone, a computer or an IoT device that is connected to the concentrator device using some of the wireless network types which can include proprietary IoT networks (LoRa, Sigfox, NB-IoT, etc.), the 3rd generation (3G)/ 4th generation (4G)/ 5th generation (5G) cellular networks, wireless local area network (WLAN) or satellite communication.

Moreover, several authentication techniques for the IoHT have been proposed in recent years to improve the security of the IoHT data transmission through securely encrypting patients' confidential medical data and transmitting it to medical advisors. To contribute to these attempts, this work proposes a lightweight blockchain-based authentication scheme that offers protection against a variety of security risks. More specifically, the main goal of this work is to ensure the efficient transfer of the confidential information of the patient to medical professionals (doctors) and to send the confidential medical prescription from the doctor to the patient through the development of a novel authentication scheme. Furthermore, secure handover authentication is suggested to avoid the re-authentication of patients when they move from one location to another.

Therefore, the main contributions of this work are:

1. Development of an authentication scheme that guarantees efficient anonymous authentication for patients and medical staff, where confidential biological information is accessed only by authenticated doctors or patients.
2. Development of an authentication scheme that guarantees integrity and data confidentiality of both the confidential biological information and medical prescription of patients and doctors from attackers.
3. Development of an authentication scheme that guarantees an efficient revoking mechanism for malicious misbehaving of medical staff in the IoHT wireless body area network.
4. Development of an efficient authentication handover that enables avoiding re-authentication of the patients when new doctors start their health monitoring process.

The rest of the manuscript is structured as follows. Section 2 describes some of the prevalent authentication schemes in IoT networks. Basic preliminaries of the methods used for the development of the proposed authentication scheme are introduced in Section 3.

The operating methodology of the proposed authentication scheme is described in Section 4. Security analysis is explained in Section 5. Performance study and comparison with other prominent IoHT authentication schemes in terms of computational, communication and storage costs are analyzed in Section 6. Finally, Section 7 concludes the manuscript.

2. Related Works

Many authors have concerted on providing an efficient, secure, anonymous protocol to provide security among IoHT users. Identification (ID)-based public key was suggested by Wang et al. in [13] where the private secret key of the user is computed by the key generator based on the identity of the user. This scheme encountered key escrow problems and vulnerability to several security assaults. Zhao et al. in [14] suggested an elliptic curve-based authentication scheme for IoHT users. However, this scheme proves to be vulnerable in securing the privacy and anonymity of IoHT users. To compensate for these drawbacks, Omala et al. in [15] suggested an authentication scheme based on remote protocol. The anonymity of the end users and security against impersonation attack is achieved in this work. Several authentication schemes based on authentication and key agreement protocol are suggested in the works [16–18]. These works mainly focus on the unlinkability between the end users and forward secrecy having the main drawback in the reply attack.

Song in [19] has developed a novel smart card-based password authentication system. Based on the upgraded smart card authentication approach, this scheme demonstrates that it is impossible for an adversary to retrieve the information. Additionally, it is challenging for an attacker to masquerade as a genuine authenticated user. In this study, the symmetric approach is used to encrypt both the server's secret key and the user's actual identity. Li et al. in [20] offer a solution for forward secrecy and password detection. The biggest disadvantage is that the user cannot change the password without the trusted authority's consent. The vulnerability of the scheme proposed in [19] was demonstrated by Chen et al. in [21], and according to demonstrated results, if the smart card is missing, it results in a password-predicting attack. Additionally, although mutual authentication between the end users is provided in [21], password detection during the login step is the primary downside. A unique RSA-based authentication technique was proposed by Sutrala et al. IN [22] to protect end users' anonymity. This work is resistant to a variety of attacks, including impersonation attacks, password-guessing attacks and reply attacks. However, as compared to other methods of a similar nature, the proposed scheme has a relatively high communication cost. Tanmoy et al. in [23] proposed an effective elliptic curve cryptography (ECC)-based smart card authentication method. In this research, user anonymity is maintained. However, this technique is vulnerable to attacks including password guessing. An authentication system based on a multi-cloud server environment was proposed by Saru et al. in [24]. This work uses biometric authentication as its foundation. Furthermore, this approach makes advantage of biohashing. According to the user's convenience, the password can be changed at any time. However, this effort does not specifically address the security issues of cloud servers. Feng et al. in [25] proposed a biometrics-based authentication method for multi-cloud server environments, which addressed the shortcomings of Saru et al. [24]. However, this technique is vulnerable to known session key attacks.

A new and enhanced smartcard-based authentication system was developed by Islam [26]. His proposed work fixes the problems authentication scheme proposed by Li et al. in [20]. However, involving the proposed procedure has a significant communication and computational cost. An improved authentication mechanism with increased security was proposed by Kaul and Awasthi in [27]. This work has proven that the proposed mechanism is safe for several potential well-known attacks, including impersonation attacks, bogus message attacks and session key assaults. However, the execution of this strategy comes at a considerable computational cost. Additionally, this technique is vulnerable to password-guessing attacks. An effective RSA cryptosystem was proposed by Amin et al. in [28] for distant user authentication. The proposed system is resistant to both active and passive attacks. However, this work is vulnerable to impersonation and password-guessing attacks. An identity-based authenticated approach was proposed by Luo et al. in [29]. Mutual authentication using a smart card is carried out in the proposed approach. However, the technique has a significant computational cost and is vulnerable to man-in-the-middle and session key attacks.

In a multi-server context, Ali and Pal in [30] have recommended a three-factor authentication system to improve security. However, there is a significant communication overhead in this approach. The technique is resistant to a variety of attacks, including biometric and session key intrusions; however, it is vulnerable to known session key attacks and lacks secrecy. A strong biometric-based authentication method was put forth by Qi and Chen in [31]. In the case of this method, security is aided by mutual authentication between the entities. The method offers full confidentiality and is resistant to denial-of-service attacks. However, the method can be used in a single-client scenario. When the same protocol is used in a multi-server context, there is a significant increase in computational and communication overhead. Additionally, this approach is vulnerable to password guessing and impersonation assaults. For telecare medicine, Sharif et al. in [32] proposed a mutual authentication system based on ECC. In this work, a novel patient authentication system and key agreement protocol are devised to provide access to the medical server. The recommended strategy defends against both aggressive and passive attacks. However, the recommended technique has a high computational cost for both server and mobile device authentication.

To overcome different security threats Xu et al. in [33] suggested a novel authentication scheme with privacy preservation. This scheme can withstand against several possible security threats such as impersonation and reply assaults. However, forward secrecy and confidentiality of the transferred information are not achieved in this work. Xiong et al. in [34] focus on the certificateless signature and encryption scheme with an efficient revoking mechanism. The computational burden due to the key updation is reviewed in this work. Though an efficient revoking mechanism is adopted, this work lacks a conditional tracking mechanism. Zhou et al. in [35] propose a certificateless key scheme that is computed based on the private key of the key generator and user. Saeed et al. in [36] focus on the certificateless online/offline signature scheme for IoHT users. Remote authentication protocol based on IoT is used in this work. The authors claim the scheme is secure against several attacks, but its vulnerability to forgery attacks is proved by Liao et al. in [37]. Ji et al. in [38] suggested a work based on big data analysis of body area networks. Conditional transmission privacy, mutual and batch authentication and un-linkability are achieved in this work. However, this work does not support handover authentication and removal of misbehaved doctors/patients. Vijayakumar et al. in [39] mainly focus on the location privacy of the end users without addressing the transfer authentication and revoking mechanisms.

Son et al. in [40] discuss the telecare medicine system. A ciphertext encryption policy is used in this work for access control of medical data. Data integrity is ensured using blockchain technology. However, there is no revoking mechanism to remove the misbehaving medical professionals or patients in the network. Zhang et al. in [41] mainly focus on the conditional privacy of the end users. The true identity of the patient is hidden in the cloud-based medical network. Moreover, the blockchain-based protocol is used for storing the data which avoids tampering with data.

Peng et al. in [42] suggested a certificateless signature scheme to overcome the resource-constraint nature of the sensor unit. The size of the signature used in this work is similar to the related prevailing works. However, this work fails to revoke the malicious end users from the medical network. Lara et al. in [43] proposed a two-party authentication scheme based on elliptic cryptography. Though this method uses the lightweight authentication protocol, there is no efficient handover and revocation mechanism in this work. Kumar et al. in [44] focus on cloud-assisted technology to improve storage capacity. Due to the limited storage capacity of the mobile unit controller, a large volume of collected data cannot be stored and analyzed. To overcome this issue, gathered data is stored in the cloud storage; however, the security of maintaining the information in the cloud is questionable. Moreover, the computational cost of this work is comparatively high.

Although presented related works show improvements in terms of the development of authentication schemes, the main research gap is the lack of authentication schemes that offer a combination of secure re-authentication of the patients (adopting a handover mechanism) and revocation of the misbehaving doctors. This paper tends to fill this gap with the introduction of a novel authentication scheme dedicated to improving authentication efficiency and reducing computing costs. In this work, this research gap tends to be fulfilled by proposing a solution that is based on the blockchain concept. Confidential information is stored in the blockchain and only authenticated IoHT users can access this data. If any intruder tries to hack the block, this will have an impact on the subsequent blocks affecting the entire blockchain network. When the patient moves from one location to another location without the involvement of a trusted authority, the new doctor takes the data of the patient from the blockchain. As a result, there is no re-authentication of the patient, which results in a reduction in the authentication time.

Moreover, a revocation mechanism is adopted in a way that when the misbehaving doctors (attackers) are identified by the trusted authority, their fake identities are loaded into the blockchain list. Hence, the misbehaving doctor will not be allowed to proceed further in the IoHT network. The results of the performance comparison in terms of computational, communication and storage overhead of the proposed authentication scheme are compared with other known state-of-the-art authentication schemes.

3. Development Methods of the Proposed Authentication Scheme

The methods on which the development of the proposed authentication scheme is based will be presented in this section and they include elliptic curve cryptography, bilinear pairing and blockchain in the IoHT network. Moreover, in this section, the analyzed system model will be presented.

3.1. Elliptic Curve Cryptography

The proposed authentication scheme exploits the concept of ECC. It is the concept of realization of public-key cryptography using the algebraic structure of elliptic curves over finite fields. Let us take an elliptic curve over a finite field demarcated by $E(i,j) : p^2 = r^3 + ir + j \; mod \; q$, which gratifies the condition $4i^3 + 27j^2 \neq 0$ and where $i, j \in Z_q^*$ under the group $G = \left\{(r,p) : r, p \in Z_q^*, (r,p) \in E\right\} \cup \{\circledcirc\}$. Here, $\circledcirc$ signifies the identity value under the additive group. Moreover, the scalar multiplication in ECC is denoted as $nA = A + A + A + A + \cdots A$, where n denotes the private key value. The scalar point addition is denoted as $A + B = (r_{3,} p_3)$ such that $A = (r_1, p_1) \in G, B = (r_2, p_2) \in G$, where the values of r_3 and p_3 are calculated as follows:

$$r_3 = \lambda^2 - r_1 - r_2 \; mod \; q \tag{1}$$

$$p_3 = (\lambda(r_1 - r_3) - p_1) \; mod \; q \tag{2}$$

and constant λ equals:

$$\lambda = \begin{cases} \frac{p_2 - p_1}{r_2 - r_1} mod \; q \; if \; A \neq B \\ \frac{3r_1^2 + i}{2p_1} mod \; q \; if \; A = B \end{cases} \tag{3}$$

3.2. Bilinear Pairing

Another relevant concept for executing the proposed authentication scheme is commonly used to construct and analyzed cryptographic systems. It is based on pairing between elements of two cryptographic groups $(G_1, \; G_2)$ to a third group with a mapping $: G_1 * G_2 \rightarrow G_T$. Let us consider G_1 and G_2 as the multiplicative cryptographic groups of prime order q. Let Z_q^* be the multiplicative group of the finite field F_p and the $e : G_1 * G_2 \rightarrow G_T$ be a bilinear map which gratifies the succeeding properties. Next properties can be achieved:

(1) Bilinearity: for any $A, B, C \in G_1$, $e(A, B + C) = e(A, B)e(A, C)$ and $e(A + B, C) = e(A, C)e(B, C)$.
(2) Non-degeneracy: for non-identify points $P, Q \in G_1$, $e(P, Q) \neq 1_{G_T}$, where 1_{G_T} is the identity point of G_T.
(3) Computability: for any two points $P, Q \in G_1$, there exists a polynomial time algorithm to determine the value of $e(P, Q)$.

3.3. Blockchain Technology

The developed authentication scheme utilizes the concept of blockchain technology. In blockchain technology, information is stored in the form of blocks that are linked together in a secure way. Any modification of data in the block will affect the subsequent blocks. Thus, the data loaded in the blocks are immutable [45–48]. In our work, confidential information is stored in the blockchain and only the authenticated IoHT users can access the data. If any intruder tries to hack the block, it will affect the subsequent blocks affecting the entire blockchain network. The medical experts are responsible for providing the medical prescription to the patient. There may be a possibility that the medical expert/doctor can be corrupted, and as a consequence, send fake data regarding the patient to the subsequent doctor in the network. This will degrade the performance of the IoHT.

In the proposed authentication scheme, the introduction of blockchain technology alleviates these problems. As an outcome, blockchain-integrated IoHT empowers authenticity and integrity, without the involvement of a trusted entity, thus decreasing the computational overhead.

3.4. System Model

The system model used for analyses is composed of three entities. Figure 1 illustrates the IoHT architecture of the analyzed system model. The three major entities of the analyzed system model are the trusted entity, the mobile control unit and the end users.

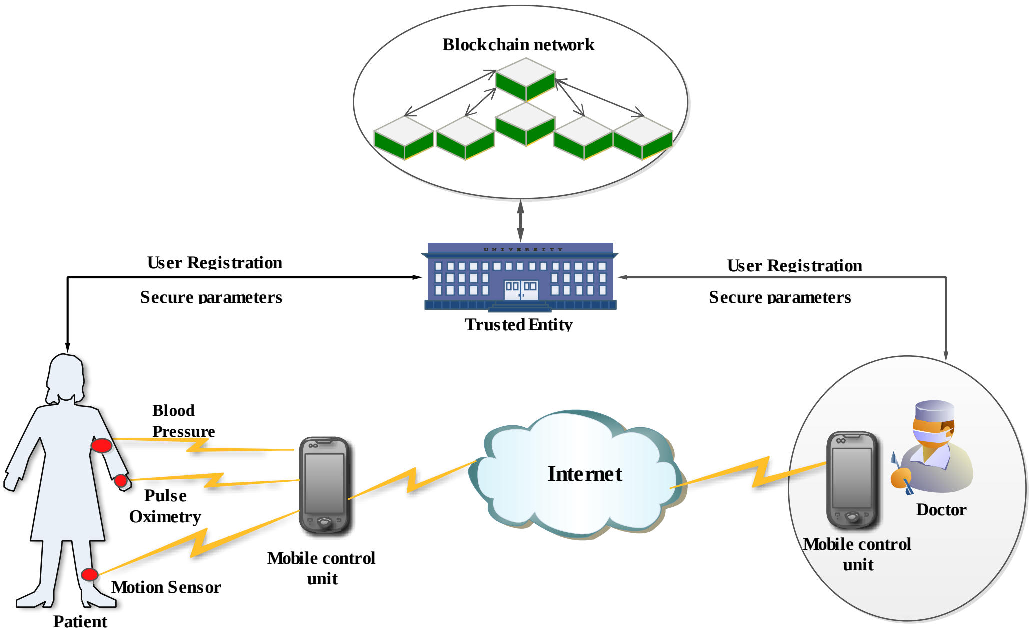

Figure 1. Proposed IoHT architecture.

The trusted entity (TE) is a completely trusted authority, and it cannot be compromised by anyone. It is responsible for generating the system parameters and providing the authentication parameters to the authenticated users in the IoHT network (Figure 1).

Initially, both the patient and medical experts should register in the TE by providing their required original credentials. After their successful registration, the required parameters are given to the authenticated users by the TE. Moreover, the TE is responsible for adding malicious doctors to the blocklist. As a result, the malicious doctors are revoked from the IoHT and their further communication in the network is avoided.

The mobile control unit (MCU) is provided to both authenticated end users in the IoHT network (Figure 1). The MCU has a high capability of performing the computation, data storage and generation of system parameters. There are two different types of MCUs provided to the patient and the medical staff (doctor(s)). The MCU provided to the medical staff has the capability of encrypting the medical prescription and sending it to the patient's device. Moreover, it will be responsible for collecting biological confidential information from the patient's MCU. The patient's MCU is embedded with a controller that is capable of collecting sensitive data from the sensors attached inside or on the body of the patient. This collected sensitive data are encrypted and sent back to the medical staff MCU (Figure 1). The patient MCU has an in-build analog to digital converter (ADC) for converting the analog sensor data collected from the sensors into digital signals and processing it in the MCU of the patient.

The end users in the IoHT network are medical staff (professionals)/experts and patients (Figure 1). To become an authorized user in the network, they should be registered in the network. Only after their successful registration, they become authenticated users. Only the authenticated users are provided with a unique MCU by the TE. With the help of the MCU, the end users communicate in the network and transfer the required information between them (Figure 1).

3.5. Security Objectives

The analyzed IoHT system model presented in Figure 1 can be susceptible to different security threats. The main security objectives can be categorized into the following five types:

- *Ensuring message integrity and authentication:* the confidential biological sensitive data of the patient or the medical prescription of the doctor should be integrity preserved. The possibility of forging or modifying the information by the intruder should be eliminated.
- *Ensuring nonrepudiation:* only authenticated end users are allowed to participate in the data transfer over the IoHT network. There must be no possibility for the registered users to deny the message transmission once it is sent.
- *Ensuring anonymity and privacy:* the real identity of the end users should be preserved during the transfer of confidential data. Moreover, the private confidential information of the end users should be preserved.
- *Ensuring unlinkability:* there should not be any correlation between the subsequent information sent between the end users.
- *Ensuring revocation and traceability:* if any mishap occurs in the network and the end user is trying to send fake information, the real identity of the end user should be traced immediately and revoked from the IoHT network.

4. Description of the Proposed Authentication Scheme

For an efficient transfer of confidential biological information between the patients and doctors in the current scenario, a blockchain-based integrity preservation scheme is proposed in this work. This scheme also achieves anonymous authentication between the end users. The notations and their description used in the further analyses are shown in Nomenclature.

The important steps that are carried out in the proposed scheme include initialization of the system, registration of both patients and doctors with a trustworthy network, Anonymous authentication, handover authentication, preservation of integrity and revocation. The entire flow diagram of the proposed authentication scheme is shown in Algorithm 1 and Algorithm 2, respectively. Algorithm 1 shows the phases related to the registration, the key generation and authentication of the patient, while Algorithm 2 shows the authentication of the doctor and handover authentication phases.

Algorithm 1: Flow diagram of registration, key generation and authentication of patient.

```
part 1: the anonymous authentication of patient
Initialization:
1. Elliptic curve of finite field: $y^2 = x^3 + ax + b \ mod \ q$
2. Points on the curve: $X$
3. Random numbers $a, b \ \in Z_q^*$
4. Public parameter of TE: $\alpha = aX$
5. Authentication parameter of TE: $\beta = bX$
6. Hash function generation: $H : \{0,1\} \to Z_q^*$
7. Public parameters: $(\alpha, \beta, H, X, e(X,X), q)$
Patient's registration:
8. TE chooses $\rho_i, k \in Z_q^*$
                    calculate $VID_{p_i} = \rho_i(a+b)$
                    calculate $FID_{p_i} \in Z_q^*$
9. $(\rho_i, VID_{p_i}, FID_{p_i}, x_1, x_3)$ $\longrightarrow$ Patient
10. $(FID_{p_i}, Z)$ $\longrightarrow$ Blockchain where $Z = e(X,X)^{\rho_i}$
Doctor's registration:
11. TE chooses $c_i, x \in Z_q^*$
                    calculate $VID_{di} = \left(\frac{1}{a+b}\right)X$
                    calculate $FID_{di} \in Z_q^*$
12. $(VID_{di}, FID_{di}, x, y_3, y_5, y_6, y_7)$ $\longrightarrow$ Doctor
Patient's key generation:
13. secret key is $Sk_{p_i} = x_3 + H(x_1 || FID_{p_i})\rho_i$
14. public validation key is $Pk_{p_i} = Sk_{p_i}.X$
Doctor's key generation:
15. secret key is $Sk_{d_i} = y_5 + H(y_1 || FID_{d_i})x$
16. public validation key is $Pk_{d_i} = Sk_{d_i}.X$
Anonymous authentication of Patient:
            Patient                                   Doctor
17. $\rho_i X$            $\longleftrightarrow$                  $FID_{di}X$
18. $FID_{di}X$                                        $\rho_i X$
19. $f = FID_{di}X.\ \rho_i$                           $f = \rho_i X.FID_{di}$
20. $f_1 = VID_{p_i} \oplus H(f)$  $\longrightarrow$   $VID_{p_i} = f_1 \oplus H(f)$
21.                                   Verifies $e(VID_{p_i}X, VID_{d_i}) = Z$
22.                                   $AA = (FID_{p_i}, FID_{d_i}, H(FID_{p_i}, FID_{d_i}))$
23. $FID_{d_i} = VID_{p_i} \oplus f_2$  $\longleftarrow$  $f_2 = VID_{p_i} \oplus FID_{d_i}$
```

4.1. System Initialization

In the phase of system initialization, an elliptic curve of finite field $y^2 = (x^3 + ax + b) mod\ q$ is chosen by the TE, where q is the largest prime value (line 1 in Algorithm 1). Let the X denote the point on the finite elliptic curve (line 2 in Algorithm 1). In the next phase, the TN chooses $a, b \in Z_q^*$ as the random numbers (line 3 in Algorithm 1). Let the Z_q^* be the multiplicative group of size q. Moreover, the public parameter and the authentication parameter are calculated as $\alpha = aX$ and $\beta = b$ (lines 4 and 5 in Algorithm 1). The system initialization phase ends with the TE publishing the parameters $(\alpha, \beta, H, X, e(X,X), q)$ to all the patients and doctors who joined the network (line 7 in Algorithm 1). Here, the hash function is given by H:{0, 1}* and $e(X,X) = g$ (line 6 in Algorithm 1). The hash function is used for ensuring data protection of an individual's privacy rights in the blockchain system.

Algorithm 2: Anonymous authentication of doctor and handover authentication.

part 2: the anonymous authentication of the doctor

```
                    Doctor                                          Patient
1.  Reception of parameters:
    $VID_{di}, FID_{di}, c_i, x, b, y_3, y_5, y_6, y_7$              $\longleftarrow$
2.  $l_1 = FID_{d_i} \bigoplus y_7$
3.  $l_2 = VID_{p_i} \bigoplus y_6$
4.          $\xrightarrow{l_1,\ l_2,\ c_i}$
5.                                                  $y_6 = VID_{p_i} \bigoplus l_2$
6.                                                  $y_7 = FID_{d_i} \bigoplus l_1$
7.                                                  Verifies $y_6 X = (y_1 + y_6 \beta)$
            Transfer of biotic information from the patient to the doctor
                    Patient                                         Doctor
8.  $t_1, t_2 \in Z_q^*$
9.  $u_1 = t_1 (Pk_{p_i} + H(\omega) X)$
10. $v_1 = H(g^{t_1} || Pk_{d_i})$
11. $m_1 = t_2 X$
12. $m_2 = [Sk_{p_i} + H(\omega)]^{-1} X - t_2 Pk_{d_i}$
13. $(u_1, v_1)$, $m_1$ and $m_2$                                   $\longrightarrow$
14.                                                 Verifies $e(u_1, Sk_{d_i}\ m_1 + m_2) = g^{t_1}$
            Transfer of medical prescription from the doctor to patient
                    Doctor                                          Patient
15. $t_3, t_4 \in Z_q^*$
16. $u_2 = t_3 (Pk_{d_i} + H(\omega') X)$
17. $v_2 = H(g^{t_3} || Pk_{p_i})$
18. $m_3 = t_4 X$
19. $m_4 = [Sk_{d_i} + H(\omega')]^{-1} X - t_4 Pk_{p_i}$
20. $(u_2, v_2)$, $m_3$ and $m_4$                                   $\longrightarrow$
21.                                                 Verifies $e(u_2, Sk_{p_i}\ m_3 + m_4) = g^{t_3}$
                         Handover authentication
                Current doctor                                  Next doctor(s)
22. $d_1,\ d_2, d_3 \in Z_q^*$
23. $D_1 = d_1 \alpha, D_2 = d_2 \alpha, D_3 = D_1 + D_2,$
    $D_4 = d_3 \alpha, D_5 = D_3 + D_4$
24. $Q_i = \partial_i (\ d_1 + d_2 + d_3) mod\ q\ where\ \partial_i = H(\omega \times D_4)$
25. $\sigma = (D_4, \omega)$
26. $\Big(Q_i, TS, \omega, \sigma, D_3, FID_{pi}\Big)$ $\longrightarrow$       $\partial_i = H(\omega \times D_4)$
27.                                                 Verifies $Q_i \alpha = \partial_i D_5$
```

4.2. Patient's Registration

The next phase of the developed authentication algorithm is the patient registration phase (Algorithm 1). Initially, the patients should be registered with the TE. Moreover, the patients should provide their confidential credentials such as an identification card, mobile number, address, etc., to the TE in an offline way. Once the credentials submitted by the patients are verified, TE chooses a random number $\rho_i, k \in$ and calculates the validation ID and fake ID for each and every patient (p_i) as VID_{p_i} and FID_{p_i}, where $VID_{p_i} = \rho_i(a + b)$ and $FID_{p_i} \in Z_q^*$ (line 8 in Algorithm 1).

To communicate with everyone, a fake identity is used. Only the fake identity is exposed to other entities during data transfer. Moreover, in the TE, dummy identities are mapped to the true identities. Even if the fake identities are captured, they provide zero information about the true identities. Thus, the authorized user can anonymously authenticate the specific user and maintain privacy. The TE computes the following parameters $x_1 = R + \rho_i X$, $x_2 = H(x_1 || FID_{p_i})$ and $x_3 = a + b + x_2 k$ (line 9 in Algorithm 1).

Finally, the TE securely provides $\left(\rho_i, VID_{p_i}, FID_{p_i}, x_1, x_3\right)$ to the patients. Moreover, the TE stores $\left(FID_{p_i}, Z\right)$ in the blockchain network, where $Z = e(X, X)^{\rho_i}$ (line 10 in Algorithm 1).

4.3. Doctor's Registration

Similar to the patient's registration, in the next phase of the proposed algorithm, it is mandatory for the doctors to register with the TE by giving the required credentials. The validation ID for each doctor is calculated as $VID_{di} = \left(\frac{1}{a+b}\right)X$ and the fake identity for every doctor is computed as $FID_{di} \in Z_q^*$ by the TN (lines 11 in Algorithm 1). Moreover, the TN chooses two random numbers $c_i, x \in Z_q^*$ and calculates the following parameters $y_1 = c_iX, y_2 = xX, y_3 = y_1 + y_2$, $y_4 = H(y_3||FID_{di})$, $y_5 = a + b + y_4c_i, y_6 = H(VID_{di} \times \alpha)$ and $y_7 = (c_i + y_6b) mod\ q$. Then, the TE provides the $(VID_{di}, FID_{di}, c_i, x, b,\ y_3, y_5, y_6, y_7)$ to the corresponding doctors (line 12 in Algorithm 1).

4.4. Patient's Key Generation

After the doctor's registration phase, the next algorithm phase that is executed is the patient's key generation phase. In this phase, the secret key and public key are generated by the authenticated patient device based on the received values of $\left(\rho_i, VID_{p_i}, FID_{p_i}, x_1, x_3\right)$. The secret key is computed as $Sk_{p_i} = x_3 + H(x_1\big|\big|FID_{p_i})\rho_i$ (line 13 in Algorithm 1) and the public validation key is calculated as $Pk_{p_i} = Sk_{p_i}.X = \alpha + \beta + H(x_1\big|\big|FID_{p_i})x_1$ (line 14 in Algorithm 1). Finally, the key pair is maintained as $\left(Sk_{p_i},\ Pk_{p_i}\right)$. Here, the public verification key is generated internally from the public and authentication parameters of TE.

Proof of validation.
$Pk_{p_i} = Sk_{p_i}.X$
$= [x_3 + H(x_1||FID_{p_i})\rho_i]X$
$= x_3X + H(x_1||FID_{p_i})\rho_iX$
$= x_3X + H(x_1||FID_{p_i})\rho_iX$
$= (a + b + x_2k)X + H(x_1||FID_{p_i})\rho_iX$
$= (aX + bX + (H(x_1||FID_{p_i}))kX + H(x_1||FID_{p_i})\rho_iX$
$= (aX + bX + H(x_1||FID_{p_i})[kX + \rho_iX]$
$= \alpha + \beta + H(x_1||FID_{p_i})[kX + \rho_iX]$
$= \alpha + \beta + H(x_1||FID_{p_i})[kX + R]$
$= \alpha + \beta + H(x_1||FID_{p_i})x_1$ □

4.5. Doctor's Key Generation

Similar to the previous phase related to the patient's key generation, in this phase, the secret key and public key are generated by the authenticated doctor's device based on the received values from the TE. The secret key is computed as $Sk_{d_i} = y_5 + H(y_1\big|\big|FID_{d_i})x$ (line 15 in Algorithm 1) and the public validation key for the doctor is calculated as $Pk_{d_i} = Sk_{d_i}.X = \alpha + \beta + H(y_3\big|\big|FID_{d_i})y_3$ (line 16 in Algorithm 1). Finally, the key pair is maintained as $\left(Sk_{d_i},\ Pk_{d_i}\right)$. Here, the public verification key is generated internally from the public and authentication parameters of TE.

Proof of validation.
$Pk_{d_i} = Sk_{d_i}.X$
$= [y_5 + H(y_3||FID_{d_i})x]X$
$= y_5X + H(x_1||FID_{p_i})xX$
$= (a + b + y_4c_i)X + H(y_3||FID_{d_i})xX$
$= (aX + bX + (H(y_3||FID_{d_i}))c_iX + H(x_3||FID_{d_i})xX$
$= (aX + bX + H(y_3||FID_{d_i})[c_iX + xX]$
$= \alpha + \beta + H(y_3||FID_{d_i})[c_iX + xX]$
$= \alpha + \beta + H(y_3||FID_{d_i})[y_1 + y_2]$
$= \alpha + \beta + H(y_3||FID_{d_i})y_3$ □

4.6. Patient's Anonymous Authentication

The next phase of the proposed algorithm is dedicated to the patient's anonymous authentication. The process of validating the credentials of patients and doctors in order to ensure security is known as authentication. The anonymous authentication process authenticates doctors and patients without disclosing their true identities. As a result, anonymous authentication protects end users' privacy. In order to communicate with patients and other doctors, the MCU of the doctors and patients should perform anonymous authentication. The steps described further are carried out in the process of the patient's authentication phase (Algorithm 1).

When the patient reaches the doctor's spot, the MCU of the patient sends $\rho_i X$ to the MCU of the corresponding doctor (line 17 in Algorithm 1). Likewise, the MCU of the corresponding doctor sends $FID_{di}X$ to the patent's MCU (line 18 in Algorithm 1). After this phase, the patient's MCU computes $f = FID_{di}X.\ \rho_i$ (line 19 in Algorithm 1). Similarly, the doctor's MCU computes $f = \rho_i X.FID_{di}$ (line 19 in Algorithm 1). Moreover, the patient's MCU calculates $f_1 = VID_{p_i} \bigoplus H(f)$ and sends f_1 to the MCU of the doctor (line 20 in Algorithm 1). Once f_1 is received, the doctor's MCU computes the validation ID of the patient's as $VID_{p_i} = f_1 \bigoplus H(f)$. As a result, the computation time is drastically reduced due to the reduction in re-authentication time.

After computing the validation ID of the patient, the doctor's MCU checks $e\big(VID_{p_i}X, VID_{d_i}\big) = Z$ in the blockchain network (line 21 in Algorithm 1). In this case, blockchain technology is used without the association of the TE. Only authenticated IoHT users can access this data since confidential information is stored in the blockchain. Attempts to hack the block by an intruder will have an impact on the subsequent blocks affecting the entire blockchain network.

Proof of validation.
$e(VID_{p_i}X, VID_{d_i}) = e(\rho_i(a+b)X, (\frac{1}{a+b})X)$
$= e(X, X)^{\rho_i(a+b)/(a+b)}$
$= e(X, X)^{\rho_i}$
$= Z$ □

Finally, the MCU of the doctor picks the fake identity of the patient FID_{p_i} from the blockchain network (line 22 in Algorithm 1), and creates the authentication acknowledgment as $AA = \big(FID_{p_i},\ FID_{d_i}, H\big(\ FID_{p_i},\ FID_{d_i}\big)\big)$. This acknowledgment will be transmitted to all the doctor's MCUs to avoid re-authentication of the patients. Moreover, doctor's MCU also computes $f_2 = VID_{p_i} \bigoplus FID_{d_i}$ and this value of f_2 is given to the patient's MCU. Thus, the patient authenticates the doctor anonymously by extracting the fake identity of the doctor as $FID_{d_i} = VID_{p_i} \bigoplus f_2$ (line 23 in Algorithm 1). With this step, the patient's anonymous authentication process ends and the patient's MCU is ready for data transfer.

4.7. Doctor's Anonymous Authentication

The doctor provides confidential information such as medical prescriptions, diagnosis data, etc., to the patient in a secure way. Hence, it is necessary for a patient to authenticate the doctor before receiving confidential information from the doctor. Trust between the patient and doctor is mandatory to receive confidential information. The process of the doctor's anonymous authentication is presented in Algorithm 2. In this procedure, the doctor's MCU receives the following parameters $(VID_{di}, FID_{di}, c_i, x, b, y_3, y_5, y_6, y_7)$ from the TN (line 1 in Algorithm 2). Based on these values, the doctor's MCU computes $l_1 = FID_{d_i} \bigoplus y_7$ (line 2 in Algorithm 2) and $l_2 = VID_{p_i} \bigoplus y_6$ (line 2 in Algorithm 2). Finally, the values of $l_1,\ l_2$ and c_i are sent to the patient's MCU (line 4 in Algorithm 2). Once, these values are received, the patient's MCU recovers $y_6,\ y_7$ and checks $y_6 X = (y_1 + y_6\beta)$ as indicated in lines 5–7 in Algorithm 2. If this condition gratifies, the patient accepts the doctor's confidential information. The values of y_7 and y_6 are recovered as $y_7 = FID_{d_i} \bigoplus l_1$

and $y_6 = VID_{p_i} \bigoplus l_2$. After the finalization of this phase, the doctor's MCU is authenticated and transferring biotic information from the patient to the doctor can be performed.

Proof of validation.
$y_7X = (c_i + y_6b)X$
$= (c_iX + y_6bX)$
$= y_1 + y_6\beta$ □

4.8. Transfer of Biotic Information from the Patient to the Doctor

In the next phase of the proposed authentication algorithm, the transfer of biotic information from the patient to the doctor starts. To send the confidential biotic information (ω) of the patient to another doctor in the network, the MCU of the patient chooses two random numbers $t_1,\ t_2 \in Z_q^*$ (line 8 in Algorithm 2) and calculates the following parameters $u_1, v_1,\ m_1\ and\ m_2$, as indicated in lines 9–12 in Algorithm 2 using the public parameters of the patient and doctor.

Once the parameters are calculated, the cipher test (u_1, v_1), m_1 and m_2 values are sent to the doctor (line 13 in Algorithm 2). The doctor checks the condition $e\big(u_1, Sk_{d_i}.\ m_1 + m_2\big) = g^{t_1}$ based on his secret key (line 14 in Algorithm 2). If the condition gratifies, then the confidential biological information (ω) of the patient is accepted, or it is discarded if the condition is not satisfied.

Proof of validation.
$e(u_1, Sk_{d_i}.\ m_1 + m_2) = e(t_1(Pk_{p_i} + H(\omega)X), Sk_{d_i}.\ m_1 + m_2)$
$= e(t_1(Pk_{p_i} + H(\omega)X), Sk_{d_i}.\ t_2X + [Sk_{p_i} + H(\omega)]^{-1}X - t_2Pk_{d_i})$
$= e(t_1(Pk_{p_i} + H(\omega)X), Sk_{d_i}.\ t_2X + [Sk_{p_i} + H(\omega)]^{-1}X - t_2Sk_{d_i}X)$
$= e(t_1(Sk_{p_i}X + H(\omega)X), [Sk_{p_i} + H(\omega)]^{-1}X)$
$= e(t_1(Sk_{p_i} + H(\omega))X, [Sk_{p_i} + H(\omega)]^{-1}X)$
$= e(X, X)^{\frac{t_1(Sk_{p_i} + H(\omega))}{Sk_{p_i} + H(\omega)}}$
$= e(X, X)^{t_1}$
$= g^{t_1}$ □

4.9. Transfer of Medical Prescription from the Doctor to Patient

The next phase of algorithm execution, based on the received biotic information of the patient, starts the process of transfer of medical prescription from the doctor to the patient. To send confidential information to the patient such as medical prescriptions (ω') prepared by the doctor, the MCU of the doctor chooses two random numbers $t_3, t_4 \in Z_q^*$ (line 15 in Algorithm 2) and calculates the $u_2,\ v_2,\ m_3$ and m_4 parameters using the public parameters of the patient and doctor according to relations presented in lines 16–19 in Algorithm 2.

Once the parameters are calculated, the cipher test (u_2, v_2), m_3 and m_4 values are sent to the patient (line 20 in Algorithm 2). The patient checks the condition $e\big(u_2, Sk_{p_i}\ m_3 + m_4\big) = g^{t_3}$ based on his secret key (line 21 in Algorithm 2). If the condition gratifies, then the confidential medical prescription (ω') sent by the doctor to the patient is accepted or else discarded. If the patient moves from one location to another location without the involvement of a TE, the new doctor takes the data of the patient from the blockchain. As a result, there is no re-authentication of the patient, and this can contribute to a reduction in the authentication time.

Proof of validation.
$e(u_2, Sk_{p_i}\ m_3 + m_4) = e(t_3(Pk_{d_i} + H(\omega')X), Sk_{p_i}\ m_3 + m_4)$
$= e(t_3(Pk_{d_i} + H(\omega')X), Sk_{p_i}\ t_4X + [Sk_{d_i} + H(\omega')]^{-1}X - t_4Pk_{p_i})$
$= e(t_3(Sk_{d_i}X + H(\omega')X), Sk_{p_i}\ t_4X + [Sk_{d_i} + H(\omega')]^{-1}X - t_4Sk_{p_i}X)$
$= e(t_3(Sk_{d_i} + H(\omega'))X), [Sk_{d_i} + H(\omega')]^{-1}X)$
$= e(t_3(Sk_{d_i} + H(\omega'))X), [Sk_{d_i} + H(\omega')]^{-1}X)$

$= e(t_3(Sk_{d_i} + H(\omega'))X), [Sk_{d_i} + H(\omega')]^{-1}X)$
$= e(X, X)^{\frac{t_3(Sk_{d_i}+H(\omega'))}{Sk_{d_i}+H(\omega')}}$
$= e(X, X)^{t_3}$
$= g^{t_3}$ □

4.10. Handover Mechanism and Integrity Preservation

In many real-life cases, the patient needs to receive medical opinions from different doctors, or specialists from different medical fields need to exchange patient medical information among them. The proposed authentication algorithm ensures authentication even for such information exchange. For instance, if the current doctor wants to share/send the confidential information of the patient (ω) to another doctor, the current doctor chooses three random numbers $d_1,\ d_2, d_3 \in Z_q^*$ (line 22 in Algorithm 2). The algorithm in the next phase computes the following values D_1, D_2, D_3, D_4 and D_5 according to relations in line 23 in Algorithm 2, and the value of the parameter Q_i according to the relation in line 24 in Algorithm 2.

Then, the current doctor sets $\sigma = (D_4, \omega)$ as the signature of a confidential biological message (line 25 in Algorithm 2). Because of the unique nature of the signature that is attached to the confidential biological message, the message's integrity will be preserved. The integrity of the signature will be preserved since it cannot be modified or altered by anyone. Then, the current doctor's MCU sends $\left(Q_i, TS, \omega, \sigma, D_3, FID_{pi}\right)$ to another doctor's MCU in the network (line 26 in Algorithm 2). Here, the TS signifies the time stamp at which the confidential message is created. Once the confidential message is received, the new doctor's MCU in the network calculates $\partial_i = H(\omega \times D_4)$ from signature and checks the condition $Q_i\alpha = \partial_i D_5$ (line 27 in Algorithm 2). If it gratifies the condition, a confidential message (ω) is accepted by the MCU of a new doctor or it is rejected if the condition is not satisfied.

Proof of validation.
$Q_i\alpha = \partial_i(\ d_1 + d_2 + d_3)\alpha$
$= \partial_i(\ d_1\alpha + d_2\alpha + d_3\alpha)$
$= \partial_i(\ D_1 + D_2 + D_4)$
$= \partial_i(\ D_3 + D_4)$
$= \partial_i D_5$ □

4.11. Revocation

Even when the authentication between users is successful, there may be a possibility that the doctors in the network may send fake information to the next doctor. In this paper, such activity is assumed as malicious misbehavior of medical staff. In that situation, the TE revokes the current misbehaving doctor from the network and marks his identity in the block list. Thus, further transmissions cannot be performed by the misbehaved doctor. For instance, let us assume that a fake message ω^* is sent by the misbehaved doctor to the other doctor in the network, i.e., the authentication parameters sent are $(TS, \omega^*, \sigma, FID_{di})$. Once these parameters are received, knowing that the message is a fake message, the new doctor sends these parameters to the TE. Upon receiving $(TS, \omega^*, \sigma, FID_{di})$, the misbehaved doctor with a fake identity will be removed.

Moreover, the TE sends a combination $(FID_{di}, H(FID_{di}, b))$ to all the doctors in the network. Upon receiving this, the doctor's MCU computes the parameter $ss = H(FID_{di}, b)$. If the parameter ss is equal to the received $H(FID_{di}, b)$, then the FID_{di} will be stored in the block list. Hence, the doctor with the fake identity $FID_{di,}$ will not be allowed to proceed further in the IoHT network.

5. Security Analysis

This section deals with the defense of the proposed authentication framework against various types of attacks. The defense mechanism of the proposed framework against different assaults is described as follows.

5.1. Impersonation Attack

In impersonation attacks, the intruder pretends to be an authorized user to perform the impersonation attack. In the IoHT network, an external attacker must find the secret parameters of the authenticated entities to carry out an impersonation attack by pretending to be an authorized user. The random numbers such as $\rho_i, k \in Z_q^*$ are chosen by the TE and are secretly provided to the patient in an offline manner. Similarly, the random values $c_i, x \in Z_q^*$ for the doctors are secretly chosen by the TE and are provided to them. Hence, it is difficult for an intruder to calculate these random numbers due to the fact that such calculation belongs to the discrete log problem. Moreover, the secret parameters such as ρ_i and FID_{di} are provided secretly to the patient and doctor by the TE in an offline manner. These values are transferred between the entities during the anonymous authentication process. Due to all these reasons, it is hard for an intruder to pretend as a real entity and trace the values. Hence, the suggested protocol can withstand impersonation attacks.

5.2. Bogus Message Attack

To perform a bogus/fake message attack, the intruder wants to create a new fake message which is similar to the original message. However, in the authentication scheme proposed in this work, each message is attached with a signature. When the current doctor is transferring the confidential biological data of the patient to another doctor in the IoHT network, i.e., during handover authentication, the current doctor sets the signature $\sigma = (D_4, \omega)$ and sends it to the next doctor (line 25 in Algorithm 2). In this case, the value of D_4 is calculated based on the value of $d_3 \in Z_q^*$, which is a random number.

Moreover, the computation of D_1, D_2 and Q_i involves the random numbers $d_1,\ d_2, d_3 \in Z_q^*$ (lines 22 and 24 in Algorithm 2). As the numbers are random in nature, it is difficult for an attacker to trace the signature and the confidential message integrity is preserved. Moreover, during the transfer of biological information of the patient to the doctor, the biological information is secured using the private key of the patient (Sk_{p_i}). Only the authenticated doctor in the network with his secret private key (Sk_{d_i}) can obtain the confidential data of the patient. Similarly, during the transfer of a medical prescription from the doctor to the patient, the information is securely transferred via the secret key of the doctor (Sk_{d_i}). In this case, only the authenticated patient with its secret key (Sk_{p_i}) can read the medical prescription. Hence, the proposed algorithm offers a defense against fake message attacks.

5.3. Message Modification Attack

To perform a message modification attack, the intruder should modify the content of the message within the stipulated time and send the modified message to the authenticated users in the network. However, in the proposed authentication scheme, the current doctor's MCU sends $\left(Q_i, TS, \omega, \sigma, D_3, FID_{pi}\right)$ to another doctor's MCU in the network (line 26 in Algorithm 2). The current doctor sets $\sigma = (D_4, \omega)$ as the signature of a confidential biological message (line 25 in Algorithm 2). Because of the unique nature of the signature that is attached to the confidential biological message, the message's integrity will be preserved. Here, the value of D_4 is computed as $d_3\alpha$ which involves random value $d_3 \in Z_q^*$ (line 23 in Algorithm 2). However, the random value is known only to the current doctor and it lasts for a short duration. The random value changes during each subsequent transfer of information between the doctors. Even though, if an intruder cracks this random value, it is still difficult to trace the subsequent transfer of data. Hence, the suggested authentication scheme is resistant to message-modification attacks.

5.4. Revocation Atack

The revocation attack is the mechanism by which the unauthenticated entity is removed from the network. In the case of a developed authentication algorithm, the end users, both the patient and doctor, are anonymously authenticated by using their fake/dummy identity. However, there may be a situation when the current doctor may be compromised and send fake information about the patient to the subsequent or other doctors in the network. In this case, the identity of the current doctor should be revealed, and his identity should be kept on the blocklist and revoked from the network. For instance, a fake message ω^* is sent by the misbehaved doctor to the other doctor in the network, i.e., $(TS, \omega^*, \sigma, FID_{di})$. Once these parameters are received, knowing that this message is a fake message, the new doctor sends these parameters to the TE. Once these parameters are received, the misbehaved doctor with the fake identity (FID_{di}) will be removed. Moreover, the TE publishes this fake ID and places it in the blocklist to avoid further transfer of information by this misbehaved doctor in the network. Thus, the other authenticated doctors in the network will avoid further communication with the current misbehaved doctor.

5.5. Non-Repudiation Attack

The non-repudiate attack is the concept of an attack in which the end users deny the acceptance of the received information. However, in the case of the authentication scheme proposed in this work, only after the successful authentication of the patient and doctor by the TE are the authenticated entities (patient/doctor) allowed to participate in the IoHT network communication. Therefore, the end users cannot repudiate after transferring the related data. Either during the transfer of biotic information of the patient to the doctor by the patient's device or during the transfer of medical prescription prescribed by the doctor to the patient, secret keys of the corresponding entities are used to hide the information. Hence, either the doctor or the patient cannot repudiate data after sending it.

5.6. Anonymity and Privacy-Preservation Attack

The proposed work uses fake identities and signatures provided by the TE for transferring confidential information between the end users. This type of security threat is a sort of man-in-the-middle attack. To communicate with entities in the IoHT, a fake identity is used by the end user. This fake identity is exposed to other entities during data transfer. Moreover, in the TN, dummy/fake identities are mapped to the true identities. Therefore, even if the fake identities are captured, it will not provide any information about the true user identities. Thus, the authorized user can anonymously authenticate the specific user and maintain privacy.

5.7. Unlinkability Attack

A lack of connectivity between the two simultaneous messages that are transferred between the end users is referred to as an unlinkability attack. The suggested scheme achieves unlinkability by the usage of short-time secret key generation during the transfer of information. During the transfer of confidential biological information (ω) of the patient to another doctor in the network, the MCU of the patient chooses two random values $t_1, t_2 \in Z_q^*$ (line 8 in Algorithm 2) and calculates the cipher text (u_1, v_1), m_1,m_2 and send it to the doctor (lines 9–13 in Algorithm 2). Here, the computation of m_2 involves the usage of a secret key (Sk_{d_i}) whose validity is for a short duration. Moreover, the values of (u_1, v_1), m_1 involves t_1, t_2 which are the random values generated only during the transfer of data at a specific time interval. Once, the transfer process is completed, the values need to be changed for further communication. Similarly, during the transfer of confidential information such as medical prescriptions (ω') prepared by the doctor to the patient, the MCU of the doctor chooses two random values $t_3, t_4 \in Z_q^*$ and calculates the cipher test (u_2, v_2), m_3 and m_4 (lines 16–20 in Algorithm 2). As these random values are periodically changed, there is complete unlinkability in the suggested authentication framework.

5.8. Sybil Attack

In a Sybil attack, one or more fake identity patients (intruders) may send spurious information regarding their biological data at the same time to the authenticated doctor in the network. As a result, the authenticated doctor becomes busy in receiving this fake information. Moreover, the doctor will not be able to serve the authenticated patient, since it becomes extremely busy. In the case of the proposed authentication scheme, to send fake information by the patient's device to the doctor, the attacker (fake patient(s)) should crack the values of ρ_i to compute f and f_1 (lines 19–20 in Algorithm 1). However, the value of ρ_i is provided to the patient in an offline way during the initial registration process by TE (line 9 in Algorithm 1). Moreover, the computation of f_1 involves VID_{p_i} (line 20 in Algorithm 1), where $f_1 = VID_{p_i} \bigoplus H(f)$. Here, VID_{p_i} is also provided to the authenticated patient by the TE. Thus, manipulating these values and sending multiple fake requests to the authenticated doctor in the IoHT is not possible and the proposed authentication scheme offers protection against Sybil's attack.

5.9. Replay Attack

In the reply attack, the information is captured during the transmission and transmitted after a certain interval of time by an external attacker. To avoid this attack, in the proposed authentication scheme a timestamp is attached during the transfer of information. More specifically, during the handover authentication phase, the current doctor's MCU sends $(Q_i, TS, \omega, \sigma, D_3, FID_{pi})$ to another doctor's MCU in the network.

Here, the TS signifies the time stamp at which the confidential information is generated. Once the confidential information is received, the new doctor's MCU in the network verifies whether $|t_j - t_i| < \triangle t$, where $\triangle t$ is the time delay between internal end users. If the time delay is unreasonable, the information is simply rejected by the new doctor's MCU. As a result, the proposed authentication method can withstand the Replay attacks.

6. Performance Analysis

The performance of the proposed authentication algorithm for the described IoHT network is analyzed in terms of computational, communication and storage costs. The brief discussion regarding each analysis is explained as follows.

6.1. Computational Overhead

Computational overhead refers to the time required to complete the cryptographic operations dedicated to the authentication of the IoHT users (i.e., patients and doctors). In this work, random computations are performed for 100 simulations and the mean time of all computations is calculated as computational overhead. The performance of the proposed authentication scheme is compared with similar state-of-the-art schemes such as those published by Kumar et al. [44], Liu et al. [49], Jegadeesan et al. [50], Debiao et al. [51] and Jia et al. [52]. The simulations are performed on the server with the next hardware characteristics (Table 1): the processor Core i7 with 16 GB RAM and the 2.20 GHz CPU frequency having the 64-bit operating system with Cygwin software containing the Pairing-Based Cryptography (PBC) library [53]. Cryptographic operations including the one point cryptographic multiplication (T_m), the one point addition (T_a), the exponential operation (T_e), the pairing operation (T_p), the hashing function (T_h), and the exclusive OR operation (T_{xor}) are involved in the calculations. The time duration for each of these calculations performed on the server with specified hardware characteristics is shown in Table 1.

Table 2 shows the comparison of the relations for the calculation of the computation time for analyzed authentication schemes. The relations enable the calculation of the authentication time costs required for the above-mentioned schemes for the comparison with the authentication time costs of the authentication scheme proposed in this work. The value of n in relations presented in Table 2 defines the number of users (public keys) participating in the authentication process.

Table 1. Time duration for cryptographic operations.

Hardware Characteristics of the Simulation Server	Cryptographic Operation	Time Duration in Milliseconds (ms)
Processor: Core i7 RAM: 16 GB Frequency: 2.20 GHz Operating system: 64-bit Software: Cygwin with PBC library	One point multiplication (T_m)	2.226
	One point addition (T_a)	0.001
	Exponential operation (T_e)	3.85
	Pairing operation (T_p)	2.91
	Hashing function (T_h)	0.0023
	Exclusive OR operation (T_{xor})	0.001

Table 2. Relations for calculation of computational time for analyzed authentication schemes.

Authentication Schemes	Authentication Time at the Patient Side (ms)	Authentication Time at Doctor Side (ms)
Liu et al. [49]	$nT_p + (n+1)T_h + (2n+1)T_e$	$nT_p + (n+1)T_e + nT_h$
Kumar et al. [44]	$(n+1)T_p + (n+1)T_h + (2n+1)T_m$	$nT_p + (2n+1)T_h + (2n+1)T_m$
Jegadeesan et al. [50]	$(n+1)T_p + (n+1)T_h + (n+1)T_m$	$(n+1)T_p + nT_h + (n+1)T_m$
Debiao et al. [51]	$(n+1)T_m + (n+1)T_h + nT_p + nT_a$	$(n+1)T_m + (2n+1)T_h + nT_p$
Jia et al. [52]	$4nT_m + nT_e + 5nT_h$	$nT_p + 5nT_m + (2n+1)T_a + 5nT_h$
Proposed work (authentication scheme)	$2nT_m + nT_h + 4nT_{xor}$	$nT_m + 3nT_{xor} + nT_h + nT_p + nT_a$

Additionally, Figures 2 and 3 present the computational overhead in terms of computation time for executing the authentication process in the case of various authentication schemes at the patient and doctor sides, respectively. The simulations are performed ranging from 20 to 100 simultaneously authenticated users. The figures clearly indicate that as the number of IoHT users increases, the computation overhead for authenticating them also increases. Concerning the relations presented in Table 2, this is the expected result since the time for performing the authentication process is directly proportional to the number n of users participating in the authentication process.

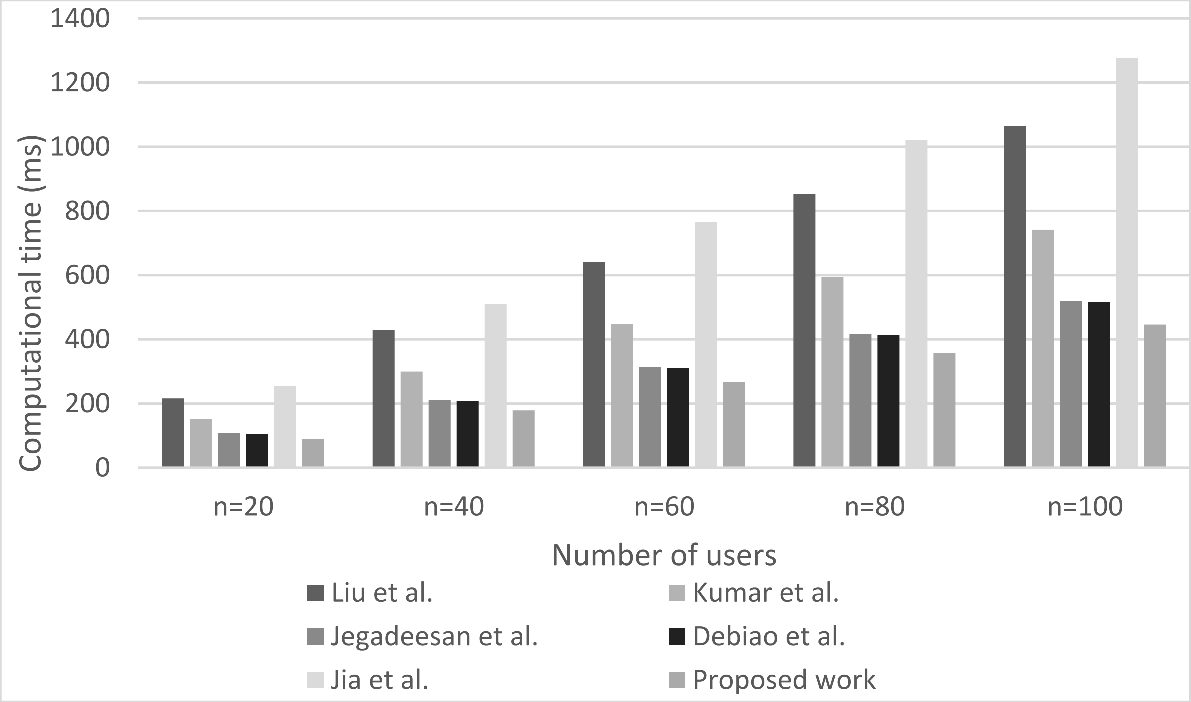

Figure 2. Computation overhead of analyzed authentication schemes at the patient's side (Liu at al. [49], Kumar at al. [44], Jegadeesan et al. [50], Debiao et al. [51] and Jia at al. [52]).

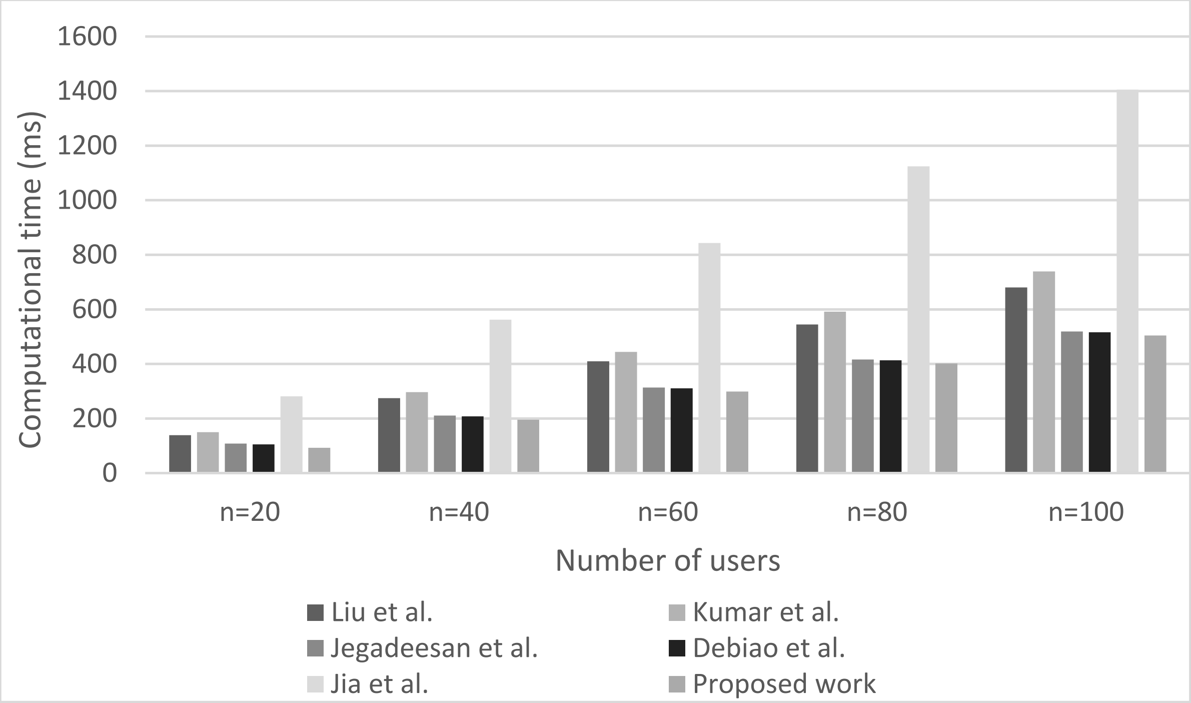

Figure 3. Computation overhead of analyzed authentication schemes at the doctor's side (Liu at al. [49], Kumar at al. [44], Jegadeesan et al. [50], Debiao et al. [51] and Jia at al. [52]).

Moreover, the results presented in Figures 2 and 3 indicate that for any number of simultaneously authenticated users, the computation time for performing the authentication process is lowest for the proposed authentication scheme. This has been achieved since the proposed authentication scheme, in contrast to other analyzed state-of-the-art authentication schemes (Table 2), involve only one hashing operation, two-point multiplication operations, and four XOR operations at the patient side for authentication purposes. For example, when compared to the other authentication schemes, the proposed authentication scheme lasts only 4.4583 ms for performing the authentication process of a single user, whereas in the case of the scheme proposed by Liu et al. in [49] is 10.65 ms, by Kumar et al. in [44] is 7.41 ms, by Jegadeesan et al. in [50] is 5.18 ms, by Debiao et al. in [51] is 5.16 ms and by Jia et al. in [52] is 12.76 ms for the authentication of the single patient. This authentication period is the lowest when compared to other analyzed state-of-the-art authentication schemes. According to Figure 3, similar results have been obtained for the computation time of analyzed authentication schemes on the doctor's side. Therefore, the results presented in Figures 2 and 3 confirm that the proposed authentication scheme outperforms other state-of-the-art authentication schemes in terms of the computation time needed for performing the authentication process.

6.2. Communication Overhead

The number of bits exchanged during the transformation of information in the frame of the authentication process between the IoHT users is referred to as communication overhead. Figure 4 shows the comparison of the communication overhead of the proposed authentication scheme and similar state-of-the-art authentication schemes such as those presented by Liu et al. in [49], Kumar et al. in [44], Jegadeesan et al. in [50], Debiao et al. in [51] and Jia et al. in [52].

Figure 4 shows that the suggested authentication scheme outperforms the authentication schemes proposed in the stated related works in terms of communication overhead. This is a consequence of the low number of bits used in the proposed authentication scheme for presenting the cipher test values. More specifically, during the transfer of the patient's biological data from the patient to the doctors, the cipher test values $((u_1, v_1)$, m_1 and

m_2) are sent to the doctor (lane 13 in Algorithm 2). Similarly, when the medical prescription is transferred from the doctor to the patient, the doctor sends the cipher test values $((u_2, v_2), m_3$ and $m_4)$ to the patient (lane 20 in Algorithm 2). The values of u_1, u_2 involve the hashing output and the public key of the patient and doctor which are computed in 160 bits. The value of v_1 and v_2 are the output of the hash function which are also computed in 160 bits. The values of m_1, m_2, m_3 and m_4 involves the hash output and the public and secret keys of the doctor and patient, respectively.

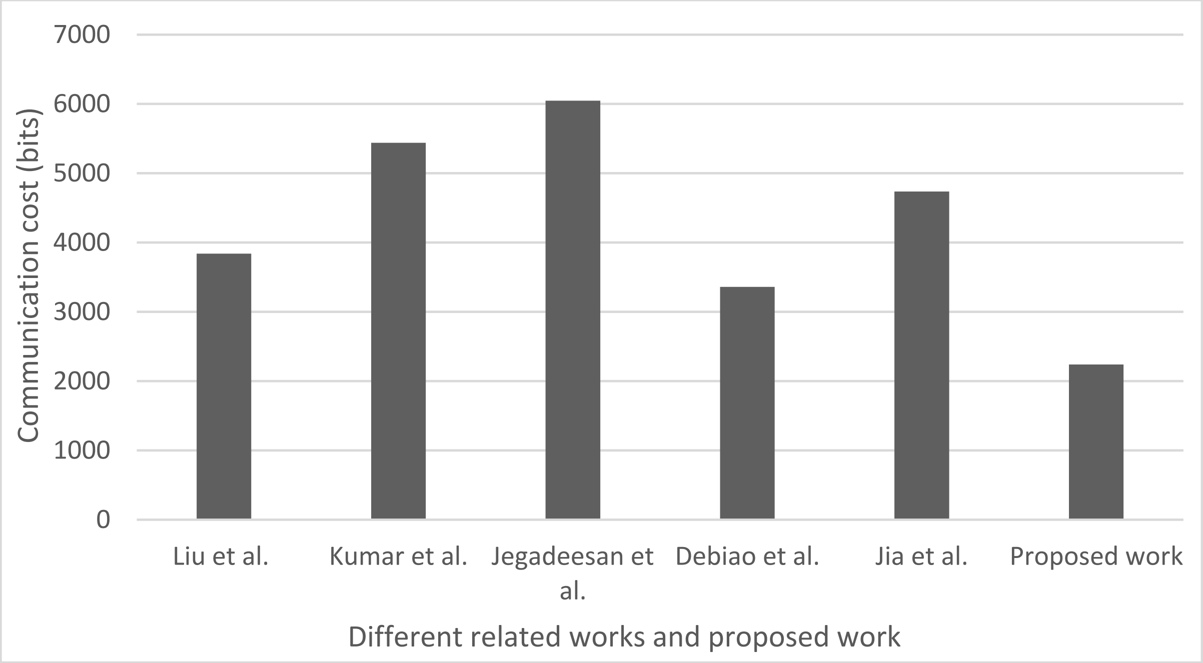

Figure 4. Communication overhead for analyzed authentication schemes (Liu at al. [49], Kumar at al. [44], Jegadeesan et al. [50], Debiao et al. [51] and Jia at al. [52]).

Therefore, the entire communication overhead of the proposed authentication scheme is computed and transferred in 2240 bits (Figure 4). When compared to the authentication costs of other authentication schemes presented in Figure 4, the proposed authentication scheme proposed by Liu et al. in [49] needs 3840 bits, by Kumar et al. in [44] requests 5440 bits, by Jegadeesan et al. in [50] needs 6048 bits, by Debiao et al. in [51] needs 3348 bits and by Jia et al. in [52] needs 4736 bits for the authentication of a single patient. Thus, the proposed authentication scheme results in significantly lower communication overhead.

The communication overhead of the proposed authentication scheme is 33,33% lower than the communication overhead of the authentication scheme having the second lowest communication overhead. This confirms the superiority of the proposed authentication scheme in terms of communication overhead when compared with other prominent authentication schemes.

6.3. Storage Cost

Storage overhead plays a key role in the performance evaluation of the authentication process. Storage costs account for the number of bits that must be stored in the memory of user devices during the authentication process. Table 3 shows the results obtained for the storage cost of analyzed authentication schemes. The number of bits stored in the patient's MCU and the doctor's MCU should be as small as possible.

In the proposed authentication scheme, the patients are required to store parameters $\rho_i, k, FID_{p_i} \in Z_q^*$. Similarly, doctors are required to store the parameters $c_i, x, FID_{di} \in Z_q^*$. To have accomplished authentification, only these parameters are sufficient to be stored by the patient and doctor MCU in the case of the proposed authentication scheme. Since these parameters are used for the key generation process, storing these values is essential for the efficient transfer of information between the doctor and patient. Thus, the storage overhead at the patient's and doctor's sides according to Table 3 is 480 bits. As a result, the overall storage cost of the proposed authentication scheme is 960 bits. For instance, the proposed authentication scheme requires only 480 bits to be stored on the patient's side for verification (Table 3), whereas the authentication scheme proposed by Kumar et al. in [44] requests 2176 bits, by Jegadeesan et al. in [50] needs 1792 bits, by Debiao et al. in [51] needs1088 bits and by Jia et al. in [52] needs 1184 bits for the authentication of the single patient.

Table 3. Storage overhead for analyzed authentication schemes.

Authentication Schemes	Patient's Side (Bits)	Doctor's Side (Bits)
Kumar et al. [44]	2176	2176
Jegadeesan et al. [50]	1792	1792
Debiao et al. [51]	1088	160
Jia et al. [52]	1184	1024
Proposed work	480	480

These results present a significant improvement when compared with the storage costs of existing schemes (Table 3). Therefore, the proposed authentication scheme improves the authentication process through the exploitation of a significantly lower amount of patient and doctor MCU memory. In comparison with other relevant authentication schemes, a notable decrease in the number of bits that must be saved during the authentication process gives a significant implementation advantage to the proposed authentication scheme.

7. Conclusions

In this manuscript, an efficient certificateless blockchain-based anonymous privacy-preserving authentication scheme is proposed. This work is mainly focused on the reliable and efficient transfer of authentication information between the doctor and patient user device in the IoHT environment. A detailed explanation of the algorithm for performing authentication in the IoHT network is presented. The authentication algorithm is based on the generation of private keys which are used in the authentication process during cipher text validation. In addition, these keys are generated based on the lightweight elliptic curve method. Blockchain technology is used as an approach for achieving efficient authentication of the patient without the involvement of a trusted entity. An efficient authentication handover mechanism is also developed in the frame of the proposed authentication scheme and this mechanism enables the transfer of the patient's data between the doctors in a secure way. Additionally, an efficient revoking mechanism is suggested to remove the potential misbehaving doctors from the IoHT network. The obtained results for the performance analyses of the proposed authentication scheme prove that the proposed authentication algorithm can withstand different possible security threats. Moreover, a performance comparison with other related state-of-the-art authentication schemes shows that the proposed authentication scheme enables significant improvements in terms of computation, communication and storage overhead.

The main limitation of the proposed authentication scheme is the dynamic increase in the patient's and doctor's data stored in the trusted authority. Since the bulk of data is stored in a trusted authority, data accessibility can become challenging when the amount of data significantly increases. However, if the fog computing concept is incorporated, patients' data can be temporarily stored closer to the authenticated doctor for frequent and faster data access. Therefore, performance analyses of this concept based on fog computing will be the main focus of future research.

Moreover, the algorithm proposed in this paper can be used in the practical implementations of an efficient mobile control unit for both, patients and doctors. As a result, the computational operations are performed in a faster way, which reduces the transmission delay of the confidential data. Thus, the speed of the authentication process at the devices in the IoHT network can be increased. Moreover, only a minimum number of bits need to be stored in the memory of end devices, which reduces the memory demand and leads to the reduced power consumption of mobile devices.

In addition, the location privacy of wireless body area network users will be one of the possible future extensions of this research work. Location privacy and security should be preserved while accessing the wireless body area network from various locations during the user's movement. Further, an automatic billing scheme for the medical prescriptions provided by the doctor for accessing the patient data can be incorporated into IoHT networks and this is also a research topic of interest. Finally, future work can be extended in different areas of applications such as education, supply chain management, vehicle ad-hoc networks and even government organizations.

Author Contributions: Conceptualization, A.S.R., A.M., M.R. and J.L.; methodology, A.S.R., A.M., M.R. and J.L.; software, A.S.R. and A.M.; validation, A.S.R., A.M., M.R. and J.L.; formal analysis A.S.R. and A.M.; investigation, A.S.R. and A.M.; writing—original draft preparation, A.S.R. and A.M.; writing—review and editing, M.R. and J.L.; visualization, A.S.R., A.M., M.R. and J.L.; supervision, J.L.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Nomenclature

Notations	**Explanation**
TE	Trusted entity
X	Point on the elliptic curve
q	Largest prime value
a, b	Random numbers of TE
α	Public parameter of TE
β	Authentication parameter of TE
H: {0, 1}*	Hash function
p_i, di	Patient and Doctor
ρ_i, k	Random numbers for patient chosen by TE
VID_{p_i}	Validation ID for the patient
FID_{p_i}	Fake ID for the patient
c_i, x	Random numbers for doctor chosen by TE
VID_{di}	Validation ID for doctor
FID_{di}	Fake ID for doctor
Sk_{p_i}	Secret key for patient
Pk_{p_i}	Public key for patient
Sk_{d_i}	Secret key for doctor
Pk_{d_i}	Public key for doctor
ω	Confidential biological information of p_i
t_1, t_2	Random numbers chosen by the patient
(u_1, v_1)& (u_2, v_2)	Cipher texts
ω'	Medical prescription of the doctor
$t_3, t_4, d_1,\ d_2, d_3$	Random numbers chosen by the doctor
σ	Signature of a confidential biological message
TS	Timestamp
ω^*	Fake message
$\oplus$	Exclusive OR operation

References

1. Movassaghi, S.; Abolhasan, M.; Lipman, J.; Smith, D.; Jamalipour, A. Wireless body area networks: A survey. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1658–1686. [CrossRef]
2. Subramani, J.; Maria, A.; Rajasekaran, A.S.; Al-Turjman, F. Lightweight Privacy and Confidentiality Preserving Anonymous Authentication Scheme for WBANs. *IEEE Trans. Ind. Inform.* **2022**, *18*, 3484–3491. [CrossRef]
3. Alzahrani, B.A.; Irshad, A.; Albeshri, A.; Alsubhi, K.; Shafiq, M. An Improved Lightweight Authentication Protocol for Wireless Body Area Networks. *IEEE Access* **2020**, *8*, 190855–190872. [CrossRef]
4. Jabeen, T.; Ashraf, H.; Khatoon, A.; Band, S.S.; Mosavi, A. A Lightweight Genetic Based Algorithm for Data Security in Wireless Body Area Networks. *IEEE Access* **2020**, *8*, 183460–183469. [CrossRef]
5. Rehman, Z.U.; Altaf, S.; Iqbal, S. An Efficient Lightweight Key Agreement and Authentication Scheme for WBAN. *IEEE Access* **2020**, *8*, 175385–175397. [CrossRef]
6. Yaqoob, T.; Abbas, H.; Atiquzzaman, M. Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3723–3768. [CrossRef]
7. Zhang, Y.; Xiang, Y.; Zhang, L.Y.; Rong, Y.; Guo, S. Secure Wireless Communications Based on Compressive Sensing: A Survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1093–1111. [CrossRef]
8. Lai, X.; Liu, Q.; Wei, X.; Wang, W.; Zhou, G.; Han, G. A survey of body sensor networks. *Sensors* **2013**, *13*, 5406–5447. [CrossRef]
9. Yuce, M.R. Recent wireless body sensors: Design and implementation. In Proceedings of the 2013 IEEE MTT-S International Microwave Workshop Series on RF and Wireless Technologies for Biomedical and Healthcare Applications (IMWS-BIO), Singapore, 9–11 December 2013; pp. 1–3. [CrossRef]
10. Appelboom, G.; Camacho, E.; Abraham, M.E.; Bruce, S.S.; Dumont EL, P.; Zacharia, B.E.; D'Amico, R.; Slomian, J.; Reginster, J.Y.; Bruyère, O.; et al. Smart wearable body sensors for patient self-assessment and monitoring. *Arch. Public Health* **2014**, *72*, 28. [CrossRef]
11. Wazid, M.; Das, A.K.; Vasilakos, A.V. Authenticated key management protocol for cloud-assisted body area sensor networks. *J. Netw. Comput. Appl.* **2018**, *123*, 112–126. [CrossRef]
12. Das, K.; Sutrala, A.K.; Odelu, V.; Goswami, A. A secure smartcardbased anonymous user authentication scheme for healthcare applications using wireless medical sensor networks. *Wirel. Pers. Commun.* **2017**, *94*, 1899–1933. [CrossRef]
13. Wang, D.; Ma, C. Cryptanalysis of a remote authentication scheme for mobile client-server environment based on ECC. *Inf. Fusion* **2013**, *14*, 498–503. [CrossRef]
14. Zhao, Z. An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem. *J. Med. Syst.* **2014**, *38*, 13. [CrossRef] [PubMed]
15. Omala, A.A.; Kibiwott, K.P.; Li, F. An efficient remote authentication scheme for wireless body area network. *J. Med. Syst.* **2017**, *41*, 25. [CrossRef] [PubMed]
16. Li, X.; Niu, J.; Kumari, S.; Wu, F.; Choo, K.-K.-R. A robust biometrics based three-factor authentication scheme for global mobility networks in smart city. *Future Gener. Comput. Syst.* **2018**, *83*, 607–618. [CrossRef]
17. Xu, Z.; Xu, C.; Liang, W.; Xu, J.; Chen, H. A lightweight mutual authentication and key agreement scheme for medical Internet of Things. *IEEE Access* **2019**, *7*, 53922–53931. [CrossRef]
18. Arasan, A.; Sadaiyandi, R.; Al-Turjman, F.; Rajasekaran, A.S.; Selvi Karuppuswamy, K. Computationally efficient and Secure Anonymous Authentication Scheme for Cloud Users. *Pers. Ubiquitous Comput.* **2021**, *25*, 1–11. [CrossRef]
19. Song, R. Advanced smartcard based password authentication protocol. *Comput. Stand. Interfaces* **2010**, *32*, 321–325. [CrossRef]
20. Li, X.; Niu, J.; Khan, M.K.; Liao, J. An enhanced smartcard based remote user password authentication scheme. *J. Netw. Comput. Appl.* **2013**, *36*, 1365–1371. [CrossRef]
21. Chen, B.L.; Kuo, W.C.; Wuu, L.C. Robust smartcard-based remote user password authentication scheme. *Int. J. Commun. Syst.* **2014**, *27*, 377–389. [CrossRef]
22. Sutrala, A.K.; Das, A.K.; Odelu, V.; Wazid, M.; Kumari, S. Secure anonymity-preserving password-based user authentication and session key agreement scheme for telecare medicine information systems. *Comput. Methods Programs Biomed.* **2016**, *135*, 167–185. [CrossRef] [PubMed]
23. Maitra, T.; Obaidat, M.S.; Islam, S.H.; Giri, D.; Amin, R. Security analysis and design of an efficient ECC-based two factor password authentication scheme. *Secur. Commun. Netw.* **2016**, *9*, 4166–4181. [CrossRef]
24. Kumari, S.; Li, X.; Wu, F.; Das, A.K.; Choo, K.-K.R.; Shen, J. Design of a provably secure biometrics-based multi-cloud-server authentication scheme. *Future Gener. Comput. Syst.* **2017**, *68*, 320–330. [CrossRef]
25. Feng, Q.; He, D.; Zeadally, S.; Wang, H. Anonymous biometrics-based authentication scheme with key distribution for mobile multi-server environment. *Future Gener. Comput. Syst.* **2018**, *84*, 239–251. [CrossRef]
26. Islam, S.H. Design and analysis of an improved smartcard based remote user password authentication scheme. *Int. J. Commun. Syst.* **2016**, *29*, 1708–1719. [CrossRef]
27. Kaul, S.D.; Awasthi, A.K. Security enhancement of an improved remote user authentication scheme with key agreement. *Wirel. Pers. Commun.* **2016**, *89*, 621–637. [CrossRef]
28. Amin, R.; Maitra, T.; Giri, D.; Srivastava, P. Cryptanalysis and improvement of an RSA based remote user authentication scheme using smart card. *Wirel. Pers. Commun.* **2017**, *96*, 4629–4659. [CrossRef]

29. Luo, M.; Zhang, Y.; Khan, M.K.; He, D. A secure and efficient identity-based mutual authentication scheme with smart card using elliptic curve cryptography. *Int. J. Commun. Syst.* **2017**, *30*, e3333. [CrossRef]
30. Ali, R.; Pal, A.K. An efficient three factor-based authentication scheme in multiserver environment using ECC. *Int. J. Commun. Syst.* **2018**, *31*, e3484. [CrossRef]
31. Qi, M.; Chen, J. New robust biometrics-based mutual authentication scheme with key agreement using elliptic curve cryptography. *Multimed. Tools Appl.* **2018**, *77*, 23335–23351. [CrossRef]
32. Ostad-Sharif, A.; Abbasinezhad-Mood, D.; Nikooghadam, M. A robust and efficient ECC-based mutual authentication and session key generation scheme for healthcare applications. *J. Med. Syst.* **2019**, *43*, 1–22. [CrossRef] [PubMed]
33. Xu, Z.; Xu, C.; Chen, H.; Yang, F. A lightweight anonymous mutual authentication and key agreement scheme for IOHT. *Concurr. Comput. Pract. Exp.* **2019**, *31*, e5295. [CrossRef]
34. Xiong, H.; Qin, Z. Revocable and Scalable Certificateless Remote Authentication Protocol With Anonymity for Wireless Body Area Networks. *IEEE Trans. Inf. Secur.* **2015**, *10*, 1442–1455. [CrossRef]
35. Zhou, Y.; Guo, J.; Li, F. Certificateless public key encryption with cryptographic reverse firewalls. *J. Syst. Archit.* **2020**, *109*, 101754. [CrossRef]
36. Saeed, M.E.S.; Liu, Q.-Y.; Tian, G.; Gao, B.; Li, F. Remote authentication schemes for wireless body area networks based on the Internet of Things. *IEEE Internet Things J.* **2018**, *5*, 4926–4944. [CrossRef]
37. Liao, Y.; Liu, Y.; Liang, Y.; Wu, Y.; Nie, X. Revisit of Certificateless Signature Scheme Used to Remote Authentication Schemes for Wireless Body Area Networks. *IEEE Internet Things J.* **2020**, *7*, 2160–2168. [CrossRef]
38. Ji, S.; Gui, Z.; Zhou, T.; Yan, H.; Shen, J. An Efficient and Certificateless Conditional Privacy-Preserving Authentication Scheme for Wireless Body Area Networks Big Data Services. *IEEE Access* **2018**, *6*, 69603–69611. [CrossRef]
39. Vijayakumar, P.; Obaidat, M.S.; Azees, M.; Islam, S.H.; Kumar, N. Efficient and Secure Anonymous Authentication With Location Privacy for IoT-Based IOHTs. *IEEE Trans. Ind. Inform.* **2020**, *16*, 2603–2611. [CrossRef]
40. Son, S.; Lee, J.; Kim, M.; Yu, S.; Das, A.K.; Park, Y. Design of Secure Authentication Protocol for Cloud-Assisted Telecare Medical Information System Using Blockchain. *IEEE Access* **2020**, *8*, 192177–192191. [CrossRef]
41. Zhang, X.; Zhao, J.; Xu, C.; Li, H.; Wang, H.; Zhang, Y. CIPPPA: Conditional Identity Privacy-Preserving Public Auditing for Cloud-Based IOHTs Against Malicious Auditors. *IEEE Trans. Cloud Comput.* **2021**, *9*, 1362–1375. [CrossRef]
42. Peng, C.; Luo, M.; Li, L.; Choo, K.-K.R.; He, D. Efficient Certificateless Online/Offline Signature Scheme for Wireless Body Area Networks. *IEEE Internet Things J.* **2021**, *8*, 14287–14298. [CrossRef]
43. Lara, E.; Aguilar, L.; García, J.A. Lightweight Authentication Protocol Using Self-Certified Public Keys for Wireless Body Area Networks in Health-Care Applications. *IEEE Access* **2021**, *9*, 79196–79213. [CrossRef]
44. Kumar, M.; Chand, S. A Lightweight Cloud-Assisted Identity-Based Anonymous Authentication and Key Agreement Protocol for Secure Wireless Body Area Network. *IEEE Syst. J.* **2021**, *15*, 2779–2786. [CrossRef]
45. Khan, A.A.; Laghari, A.A.; Liu, D.-S.; Shaikh, A.A.; Ma, D.-D.; Wang, C.-Y.; Wagan, A.A. EPS-Ledger: Blockchain Hyperledger Sawtooth-enabled distributed power systems chain of operation and control node privacy and security. *Electronics* **2021**, *10*, 2395. [CrossRef]
46. Siyal, A.A.; Junejo, A.Z.; Zawish, M.; Ahmed, K.; Khalil, A.; Soursou, G. Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. *Cryptography* **2019**, *3*, 3. [CrossRef]
47. Dospinescu, O.; Caramangiu, M.E. The key success factors for an M-learning cryptocurrency application. *Inform. Econ.* **2018**, *22*, 14–24. [CrossRef]
48. Zhang, J.; Wu, M. Blockchain use in IOT for privacy-preserving anti-pandemic home quarantine. *Electronics* **2020**, *9*, 1746. [CrossRef]
49. Liu, J.; Zhang, Z.; Chen, X.; Kwak, K. Certificateless remote anonymous authentication schemes for wirelessbody area networks. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *25*, 332–342. [CrossRef]
50. Jegadeesan, S.; Azees, M.; Babu, N.R.; Subramaniam, U.; Almakhles, J.D. EPAW: Efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (IOHTs). *IEEE Access* **2020**, *8*, 48576–48586. [CrossRef]
51. Debiao, H.; Zeadally, S.; Kumar, N.; Lee, J.-H. Anonymous authentication for wireless body area networks with provable security. *IEEE Syst. J.* **2017**, *11*, 2590–2601.
52. Jia, X.; He, D.; Kumar, N.; Choo, K.R. A provably secure and efficient identity-based anonymous authentication scheme for mobile edge computing. *IEEE Syst. J.* **2020**, *14*, 560–571. [CrossRef]
53. Cygwin: Linux Environment Emulator for Windows. Available online: https://www.cgywin.com/ (accessed on 24 August 2022).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.