Hindawi
Security and Communication Networks
Volume 2022, Article ID 2793116, 12 pages
https://doi.org/10.1155/2022/2793116

Research Article

An Anonymous Blockchain-Based Authentication Scheme for Secure Healthcare Applications

Arun Sekar Rajasekaran and M. Azees

Electronics and Communication Department, GMR Institute of Technology, GMR Nagar, Rajam, 532 127, Srikakulam District, Andhra Pradesh, India

Correspondence should be addressed to M. Azees; azeesmm@gmail.com

Received 7 December 2021; Accepted 17 January 2022; Published 11 February 2022

Academic Editor: Irshad Azeem

Nowadays, continuous monitoring of a patient's healthcare data has become a critical factor in human well-being. However, with the rapid advancement of wireless technology, doctors and healthcare professionals can monitor the patient's healthcare data in real time. But to access the confidential patient's data which is transferred through the open wireless medium, the secure transmission plays an important role. In this work, the privacy and the anonymity of the end-users (patient/doctor) are preserved using an anonymous blockchain-based authentication scheme. Moreover, in this work initially, mutual authentication is performed between the end-users, followed by encryption and decryption of confidential data. In addition, to avoid reauthentication of the patient again during the movement of a patient from one doctor to another, a transfer authentication protocol is performed between the doctors which enhances performance analysis. The security analysis section illustrates the withstanding capability of the proposed work against various vulnerable attacks. Finally, performance investigation of the proposed work reveals a reduction in computational and communication costs when compared to existing related works.

1. Introduction

Wireless body network [1], also referred to as body sensor network, is a network connecting various nodes such as electronic sensors and actuators, which can be wearable or embedded in a fixed position on the body or under the pores of the skin. Wireless body area network (WBAN) technology was first developed based on the knowledge of wireless personal area network (WPAN) in 1995 to communicate around the human body. It took nearly six years to develop the technology known as "BAN," which refers to communication that occurs entirely within, on, or around the human body [2].

WBAN networks can be used in remote health monitoring, medicine, multimedia, sports, military, and a variety of other fields. Extending this technology into different fields can help with the exchange of information between people or between machines and people. Wireless body network initial applications are mainly in the healthcare sector [3]. The health parameters of the patients suffering from severe diseases such as asthma, heart attack, diabetes, etc., are monitored continuously. WBAN technology gateways enable wearable computing devices to connect over long distances. By using these gateway devices, the computing devices which are on the surface or inside the human body can be connected to the Internet. In this way, doctors can access patient data from anywhere and at any time via the Internet, regardless of the patient's or doctor's location.

The WBAN device can be used to communicate with the hospital to alert them when the parameters in the patient's body vary and require assistance from the hospital. The data collected by using the computing devices of the WBAN system plays a key role in the treatment of the patient. So a high quality of data is required to ensure an accurate decision. Moreover, if a large volume of data is generated by the system, then it is necessary to manage and maintain this data securely. In addition, various standards like Bluetooth, Wi-fi, Zigbee, and so on are used for data exchange [4]. In this case, the system must be scalable, efficiently migrate between networks, and provide seamless connectivity.

Consumers are expecting low costs health monitoring systems with high-level functionalities. This is satisfied by WBAN system implementations as they are cost-optimized. But, the WBAN system's performance should be reliable even though they are cost-optimized. Moreover, the wireless links should be strong enough to accurately calibrate the measurements, even when the system is switched off/switched on. This shows the consistency of the system.

Since the data is transferred over an open communication channel, security and privacy in the system are critical and appropriate action should be taken to protect data from reaching unauthorized users. The data collected from each patient should be transferred to the doctor's end, without mixing up with other patients' data which is to be ensured. WBAN security requires authentication, confidentiality, integrity, data update, availability, and security management [5–7]. The IEEE 802.15.6, which is the most recent WBAN standard, attempts to afford security in WBAN, even though it has numerous security issues.

As the number of patients increases daily, continuous monitoring of patients' health is difficult, because patients rely entirely on doctors and other healthcare professionals, making it impossible to process all of the data at once. Even though WBAN technology helps in processing a large amount of data, security plays a key role during continuous health monitoring of patients and the processing of data. A patient's health can be also monitored by installing sensors inside the body or on the outer surface of the patient's body. Physiological parameters such as oxygen level, blood pressure, pulse, ECG, etc. are recorded and this data is transmitted to the doctor or the nursing staff who monitors the patient's health. During transmission of data from the patients to the doctor or vice versa, the information content should not be modified. Therefore security plays an important role. The data must be encrypted during transmission and decrypted at the receiver end for proper diagnosis and medication [8]. Various data collected from different patients from different areas are stored in the database, and this database must be regulated by authentication. The authenticated exchange of information reduces the potential for data abuse.

The collected data can be intelligently monitored using the Internet of things (IoT). Due to technological advancements, doctors' data now faces new security and privacy risks. The data collected may contain highly sensitive medical information. The information sent by the doctor/patient is easily intercepted and captured by adversaries due to insecure network connections. To address the aforementioned security threats, this paper introduces a physically secure blockchain-based lightweight privacy-preserving anonymous authentication scheme for WBAN. Initially, mutual authentication occurs between the patient and the doctor in the proposed framework. Finally, patients are given a unique token to prove their authenticity. When a patient moves to a different doctor in a different location, frequent authentication for verifying the patient's identity consumes more computation and communication overhead, affecting system performance. As a result, to avoid frequent authentication and to reduce computation and communication overhead, a transfer authentication protocol is proposed in this work. Furthermore, the blockchain [9] is used to keep track of patient parameters and user authentication information and to maintain the doctor's trustworthiness.

The research work's main contribution is as follows.

(i) To propose a privacy-preserving blockchain-based lightweight mutual authentication scheme for both the patient and doctor.

(ii) To perform encryption and decryption of confidential data (i.e., biotic statistics data of patient and medical prescription of doctor) to ensure confidentiality.

(iii) To propose a transfer authentication protocol by sharing the identity code of the patient to the new doctor. Hence, there is no need for the new doctor to reauthenticate the patient once again.

(iv) To develop a conditional tracking mechanism for the end-users (doctors/patients) by the medical network. Thus, the medical network will revoke the misbehaving or compromised end-users from the network.

The rest of the research is organized accordingly. The review of relevant work is provided in Section 2. Preliminary steps and system models are discussed in Section 3. Section 4 describes the proposed framework. The security analysis of the proposed framework is explained in Section 5. Section 6 discusses the effectiveness of the proposed scheme in terms of performance. The concluding tasks are presented in Section 7.

2. Related Works

The smart physical sensors accumulate and progress sensitive data from the patient body. The security, reliability, and trustworthiness of sensitive data collected and processed by smart physical sensors are critical as they are related to the welfare of human beings. Some of the related works related to the security of WBAN are discussed as follows. Liu et al. [10] proposed a scheme based on the certificateless signature. The anonymity of the end-user is preserved by the network manager. However, this scheme suffers from a lack of traceability of confidential information. Ibrahim et al. [11] proposed a scheme where the anonymity of the patient's sensor is preserved. In this work, mutual authentication takes place between the end-users in a secured way. However, the confidentiality of the user data is not preserved.

Zhao et al. [12] proposed a healthcare oriented blockchain scheme. In this scheme, blockchain is used for preserving the patient's data. Though blockchain is considered a public network, there may be a possibility of attackers gaining access to confidential data. But, here the data is stored in the form of a public address and it is difficult for an attacker to corrupt the data. Moreover, the scheme is suitable for storing a large volume of information. However, there is no transfer authentication protocol followed for the transfer of confidential information of the patients from one doctor to another doctor. Thus the computational complexity increases in this scheme. Debiao et al. [13] proved the possibility of impersonation attacks in the existing anonymous authentication schemes. The security provided by this scheme is high enough to withstand impersonation attacks. But the confidentiality and traceability of the confidential data are not addressed in this scheme.

Li et al. [14] proposed an unlinkable, confidentiality preserving authentication scheme for WBAN users. The patient's authenticated data is collected by the sensor nodes and they are transmitted to the required end-users anonymously. Though confidentiality and anonymity are preserved, the computational cost for authenticating the patients is high. Moreover, the patients need to be authenticated again when they move to the new doctors. Thus the performance analysis of the scheme is degraded. Li et al. [15] proposed a more secure authentication scheme based on a single round method to avoid the drawbacks in Liu et al. [10]. Security analysis is performed based on both informal and formal methods. Though the communication cost is reduced in this scheme, it does not provide traceability of patients' confidential data. Luo et al. [16] proposed a new privacy protector scheme for an IoT-based healthcare environment. A new type of coding method named Slepain-Wolf is used in this scheme. To prevent data loss, the self-repairing protocol is employed in this scheme. However, truly speaking the confidential data loss cannot be compromised. The summary of related works is tabulated in Table 1.

Shen et al. [17] proposed cloud-based authentication protocol for healthcare applications. Since the storage of data forms a key factor, a large volume of data can be stored only with the help of cloud-aided system. Since the storage of confidential data takes place in the cloud, the scheme is vulnerable to different types of security threats. Li et al. [18] proposed an authentication scheme based on IoT. This scheme can withstand replay attacks and message modification attacks. However, there is no transfer authentication protocol. Deebak et al. [19] proposed a scheme based on hash-based RFID. However, the scheme is vulnerable to several security threats. Alzahrani et al. [20] proposed an effective, safe, and anonymous WBAN valid key agreement protocol. Though the privacy of the user is preserved in this work, it lacks the confidentiality of the information transferred. Jabeen et al. [21] proposed a scheme for the protection of data based on a genetic algorithm. But the complexity of the algorithm leads to an increase in the computational cost analysis. Rehman et al. [22] proposed an authentication protocol based on a reliable base node. A three-level topology is used for the key agreement scheme. This protocol is free from several attacks like compromise attacks and impersonation attacks. Amjad et al. [23] proposed a work based on an optimization problem. A gamma distribution function is used to continuously monitor the health conditions of the patients. The energy optimization algorithm is used to preserve the energy consumption during the transfer of data in the form of packets. This algorithm does not deal with the relative authentication or the security of data during transmission. Kumar et al. [24] proposed an efficient scheme based on trust assessment without encryption techniques. Moreover, trust evaluator, attack-resistant features are incorporated in this work. In addition, trust is developed on the data received from the sensor and the efficiency obtained through this work is noteworthy. Lara et al. [25] proposed a Two-Party Authentication scheme. Here public keys are generated based on ECC. Since ECC is used, the computational cost for executing this scheme is notable. Though the performance analysis of this work is notable, the end-users need to be authenticated every time. Ning et al. [26] proposed a monitoring mechanism for the patients based on 5G technology. Moreover, a cost-efficient monitoring mechanism for the patients located in the home is embarked. The basic security features like authentication and privacy are not focused on in this work. Kumar and Chand [27] proposed a scheme based on cloud computing. This work mainly focused on the large resource allocation for the data received from the patients. Since the sensors used in the patients are resource-limited, they cannot store a large amount of information. Hence an efficient protocol is designed in this work. But this scheme suffers from privacy leakage and security threats. Guo et al. [28] proposed a homomorphic cryptosystem architecture. This work is mainly focused on the real-time health monitoring of the patients. Moreover, the Diffie-Hellman key exchange protocol is used to ensure security. But mutual authentication between the end-users is not provided in this work.

3. System Overview

The basic concept regarding the system model architecture and bilinear pairing is explained in the succeeding section.

3.1. System Model Architecture. A brief view regarding the proposed system model architecture and transfer authentication protocol is depicted in Figures 1 and 2, respectively. The system model is unique. In this model, there are three main entities, namely, medical network, data sensor regulator, and end-users (doctor/patient). The role of each entity is unique in nature. The medical network acts as the centralized trusted third party network and it is responsible for the initial offline registration of both patients and doctors. Moreover, it provides the required credentials to the end-users. The role of data sensor regulator is not only to collect the sensitive data from the patients but also to store the data, providing the data to the doctors in an encrypted way. In addition, reauthentication is not required in our proposed system as blockchain is utilized to store the confidential data of the patient.

*3.1.1. Medical Network (*MN*). MN* is considered as the fully trusted authority. It is responsible for the generation of public parameters, initialization of the system, registration of

Table 1: Summary of different existing works.

Existing works	Publication year	Techniques	Drawbacks
Liu et al. [10]	2014	Certificateless signature scheme	Lack of traceability of confidential information
Ibrahim et al. [11]	2016	Anonymity preservation of the patient's sensor	Confidentiality of the user data is not preserved
Zhao et al. [12]	2016	Healthcare oriented blockchain scheme	No transfer authentication protocol
Debiao et al. [13]	2017	Authentication with provable security for WBAN	Confidentiality and traceability of the confidential data are not addressed
Li et al. [14]	2017	Unlinkable, confidentiality preserving authentication scheme	Computational cost for authenticating the patients is high
Li et al. [15]	2017	Single round method scheme for BAN	Lacks traceability of patient's confidential data
Luo et al. [16]	2018	Privacy protector scheme for IoT-based healthcare	Confidential data loss
Shen et al. [17]	2018	Cloud-based authentication protocol for healthcare	Vulnerable to different types of security threats
Li et al. [18]	2018	RFID based authentication	Message eavesdropping and tag forgery attack
D. Deebak et al. [19]	2019	RFID authentication based on hash	Denial of service and data forgery attack
Alzahrani et al. [20]	2020	Anonymous WBAN valid key agreement scheme	It lacks confidentiality of the information transferred
Jabeen et al. [21]	2020	Genetic algorithm based scheme	Increase in the computational cost analysis
Rehman et al. [22]	2020	Authentication scheme based on reliable base node	Several attacks like compromise attack and impersonation attack
Amjad et al. [23]	2020	Optimization scheme for WBAN	Relative authentication or the security of data during transmission is not discussed
Kumar et al. [24]	2021	Trust assessment without encryption techniques	Complexity increases due to trust evaluator
Lara et al. [25]	2021	Two-party authentication scheme	The end-users need to be authenticated every time
Ning et al. [26]	2021	Edge computing 5G scheme	Authentication and privacy are not focused
Kumar and Chand [27]	2021	Cloud computing scheme for WBAN	Privacy leakage and security threats
Guo et al. [28]	2021	Homomorphic cryptosystem scheme	Mutual authentication between the end-users is not provided

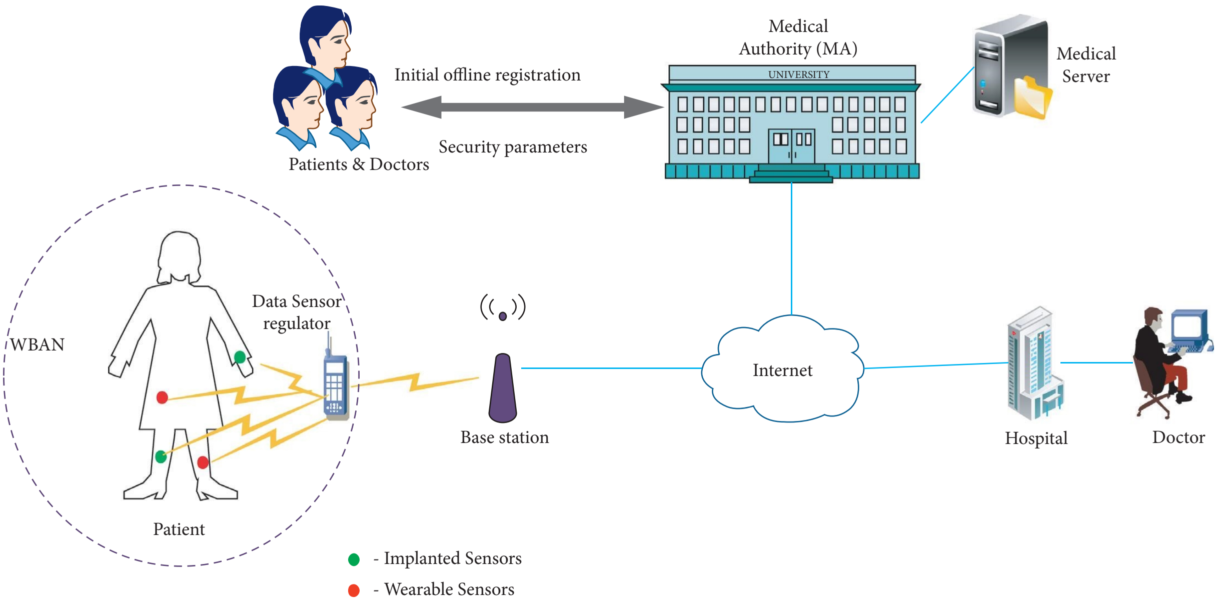

Figure 1: Proposed system model architecture.

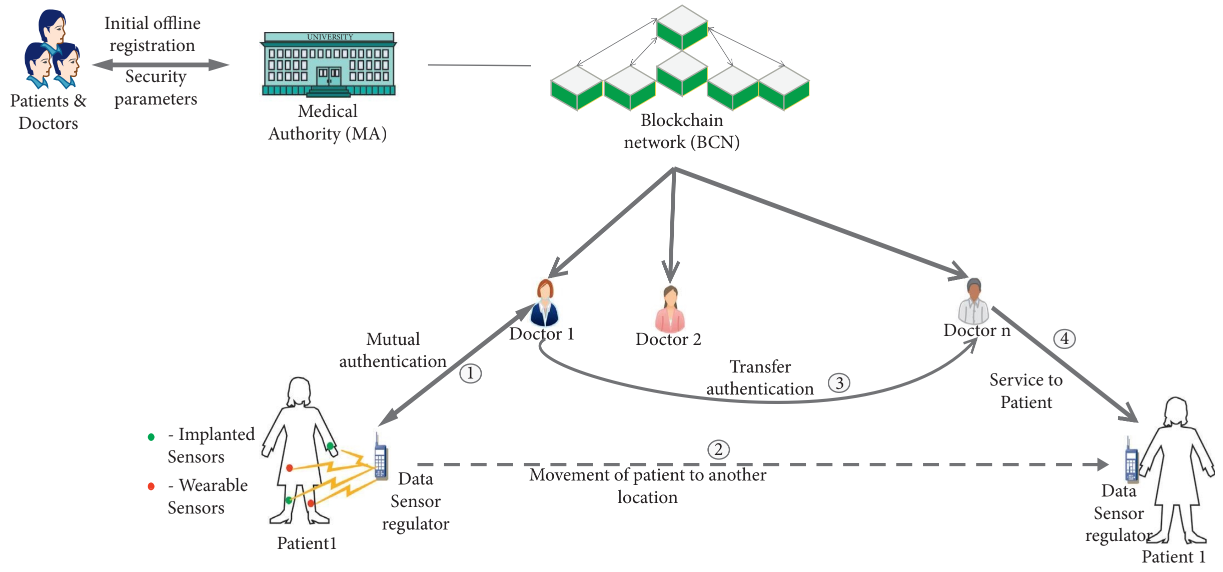

Figure 2: Transfer authentication protocol of proposed scheme.

the end-users, and the key generation for the end-users. Initially, all the end-users should register in the trusted MN by giving their confidential credentials. Once the registration is successfully performed, the MN issues the required credentials to the authenticated end-users.

3.1.2. Data Sensor Regulator. Normally, the patient is provided with two types of sensors. The sensors may be present on the surface of the body or may be implanted inside the body. The information or the data collected from these sensors are transmitted through the data sensor regulator to the required doctor through the open wireless medium. The data sensor regulator is designed to perform the communication and computation efficiently. Moreover, it is provided with random access memory (RAM) for data storage. The data collected from the MN and the required internal data of the patient are retained in the data sensor regulator. In addition, the regulator has the capability of storing the data in an encrypted way which prevents the intruder from accessing the original content of the data.

3.1.3. End-Users. The end-users may be either the doctor or the patient. The MN provides the required keys and credentials to the authenticated end-users. In addition, the keys generated by the end-users are used for mutual authentication between them. Moreover, the biotic statistics of the patient and the confidential medical prescription of the doctors are encrypted and securely transferred with the help of these keys which prevents illegal injection of data from the intruder.

3.2. Bilinear Pairing. Let G_x, G_y, and G_z be the cyclically multiplicative groups of order q.The generators of the groups G_x and G_y are represented as g_x and g_y, respectively. The isomorphism ∇ for these groups is represented as $\nabla(g_y) = g_x$. The bilinear map e: $G_x \times G_y \longrightarrow G_z$ satisfies the following properties.

Bilinearity: $e(g_{\mathrm{x}}^{\rho}, g_{\mathrm{y}}^{\sigma}) = e(g_{\mathrm{x}}, g_{\mathrm{y}})^{\rho\sigma}$, $g_x \in G_x \& g_y \in G_y$ and $\forall x, y \in Z_q^*$

Nondegeneracy: $e(g_x, g_y) \neq 1_{G_z}$

Computability: the bilinear map e: $G_x \times G_y \longrightarrow G_z$ and isomorphism ∇ are computable

4. Proposed System

In this work, blockchain-based anonymous authentication for WBAN is proposed. Initially, mutual authentication takes place between the patient and the doctor in an anonymous way. Initially patient and the doctor should perform offline registration with the medical network (MN). The MN preserves the private information of the patients and doctors in a secured manner. Moreover, MN maintains a tracking list that contains the real and dummy identity of the doctors and patients. In case of any dispute, MN will revoke the particular patient or doctor from the network with the help of the tracking list. In this work, MN is linked with the blockchain network along with the doctors. Once the initial registration of the doctors and patients with MN is completed, MN issues the required identity code (IC) and dummy identities to the end-users (doctors and patients). Based on the IC, the doctors will authenticate the patients using the distributed ledger of the blockchain network. So, if the intruder tries to acquaint with any security threats, the same will be reflected in the distributed ledger. MN reports the change in the block hash value and the particular end-user (intruder) is revoked from the network. In the suggested scheme, once the mutual authentication process is completed between the doctors and patients, transfer authentication protocol takes place between the doctors. For instance, if the patient moves from one doctor to another doctor, there is no need for the current new doctor to authenticate the patient once again. The required authentication parameters of the patient are transferred between the previous and the current doctor. Thus, the performance analysis of this work is well esteemed.

4.1. System Initialization. Initial registration is performed by the medical network offline. Both the doctors and patients should initially register in the medical networks by providing their required credentials like ID proof, mobile number, etc. through offline mode. The MN chooses two random numbers s,t as its master key and private key such that $s,t \in\in Z_q^*$. Based on these keys, the public key and the conditional parameter are generated by MN. The public key is represented as $PU_{MN} = g_x^{t+s}$ and the conditional parameters are represented as $A_1 = g_x^{1/s+t}$. Moreover, the secure one-way hash function is given by $H(\cdot)$. Finally, the MN broadcasts the system parameters as $(G_x, G_y, H, e, q, g_x, g_y, PU_{MN})$.

4.2. End-User Registration. Initially, both the patient and the doctor should perform offline registration with MN by providing their credentials.

(1) The MN picks random numbers $a_i, r, y_1, y_2 \in Z_p^*$ such that the public key is calculated as $PU_{pa} = g_x^{a_i}$. In addition, session key for the patient is calculated from the public key of the doctor as $S_{pa} = PU_D^{a_i}$. Moreover, the decryption key for the patient is provided by MN as $\beta = g_x^{1/a_i}$

(2) The dummy identity of the patient is calculated as $DI_{pa} = g_x^{a_i+t+s}$. Moreover, MN also calculates $\wp_{i\,d} = g_x^{t+y_1+y_2}$, $X = g_x^{-(y_1+y_2)}$, $Y = g_x^{s+y_1-y_2}$, $Z = g_x^{y_2-y_1}, R_1 = g_x^r$, $S_1 = g_x^s$, and $T_1 = g_x^t$. These parameters are provided to the patient and doctors.

(3) In addition, the identity code for each patient is generated by MN as $IC(t) = \sum_{i=1}^{n} u_i v_i / n$ where u_i is the identity value generated by MN for the patient. v_i is the identity value of the patient given by the patient to MN. n is the number of patients in the network.

(4) The IC and DI_{pa} are concatenated and kept in the blockchain network. In addition, IC is encrypted and broadcasted to the remaining MN in the system. So, whenever updation occurs in IC, the MN also updates its data list.

(5) MN maintains a tracking list for the patient as $(PU_{pa}, TR_{pa}, DI_{pa})$, where $TR_{pa} = g_x^{t+a_i}$. This tracking list is used to revoke the misbehaving patient from the WBAN by MN.

(6) Similarly, MN chooses a random number for b_i and d_i as its master key and private key for the doctor and computes the session secret keys $S_D = g_x^{b_i}$ and $S_{D,1} = PU_{pa}^{d_i}$.

(7) Moreover, MN calculates the public key for the doctor as $PU_D = g_y^{d_i}$ and $PU_{D,1} = g_y^{b_i}$. In addition, decryption key for the doctor is $\propto = g_y^{1/d_i}$ and conditional parameter $A_D = g_x^{t-d_i}$.

(8) The dummy identity and the tracking identity of the doctor are calculated as $DI_D = g_y^{d_i+t+s}$ and $TR_D = g_y^{d_i+t}$. MN maintains the tracking list for the doctor as (DI_D, TR_D, PU_D). The tracking list is used to revoke the misbehaving doctor from the WBAN.

4.3. Patient's Key Generation. Mutual authentication should take place between patients and doctors before the start of transferring the authenticated data. The data sensor regulator of the patient selects $q_j = g_y^{\theta_j}$ as the short time public key, where θ_j is the short time private key such that $\theta_j \in Z_p^*$ and $j < p$. Then the patient's data sensor regulator chooses four random numbers $(\mu_1, \mu_2, \mu_3 , \mu_4) \in Z_p^*$ and computes $\varnothing_0$, $\varnothing_1$, $\varnothing_2$, and $\varnothing_3$, where $\varnothing_0 = \mu_1 + 2\theta_j$, $\varnothing_1 = R_1^{\mu_1+\mu_3-\mu_4}$, $\varnothing_2 = R_1^{\mu_3+\mu_4}.S_1^{\mu_1+\mu_2-\mu_4}$, and $\varnothing_3 = R_1^{\mu_1+\mu_3-\mu_4}.S_1^{\mu_2+\mu_4}/T_1^{\mu_3+\mu_4}$.

4.4. Patient's Certificate Generation. The patient's data sensor regulator calculates the dummy parameters $\partial_1 = \theta_j - \mu_2$, $\partial_2 = \theta_j - \mu_3$, $\partial_3 = \theta_j + \mu_4$ and acceptor key as $Ak = H\ (\wp_{i\,d} \| T_1 \| S_1 \| X \| \varnothing_1 \| \varnothing_2 \| \varnothing_3 \| Z \| q_j)$. Moreover, the certificate for the patient is generated as $\text{cer}_{pa} = (\wp_{i\,d} \| Ak \| q_j \| \varnothing_0 \| \partial_1 \| \partial_2 \| \partial_3 \| X \| Y \| Z)$. Then the data sensor regulator calculates $zz = H(\text{cer}_{pa})$ and $yy = (\text{cer}_{pa} \| zz \| TS)$ where TS represents the current time stamp.

4.5. Patient's Signature Generation. To preserve the integrity of the information, patient's data sensor regulator generates the signature as $\text{sig}_{pa} = g_x^{1/H(DI_{pa})+\theta_j}$. Finally, the message is generated and sent to the doctor as $\text{mess}_{pa} = (DI_{pa} \| q_j \| yy \| \text{sig}_{pa})$.

4.6. Patient's Certificate Verification. Moreover, from the received message, the doctor checks the validity of the time stamp to avoid reply attack. If the timing value is less than the mutually agreed timing delay between the doctor and the patient, then the doctor accepts the message, else rejects it. Then, the doctor computes the parameters $T_1', S_1', \varnothing_1', \varnothing_2'$, and $\varnothing_3'$ such that $T_1' = \wp_{i\,d} \times X$, $S_1' = Y \times\ Z$, $\varnothing_1' = Y \times = R_1^{\varnothing_0-\partial_2-\partial_3}$, $\varnothing_2' = R_1^{\partial_3-\partial_2}.S_1^{\varnothing_0-\partial_1-\partial_3}$, and $\varnothing_3' = R_1^{\varnothing_0-\partial_2-\partial_3}.S_1^{\partial_3-\partial_1}/T_1^{\partial_3-\partial_2}$. Finally, doctor computes the doctor's acceptor key as $Ak\prime = H\ (\wp_{i\,d} \| T_1' \| S_1' \| X \| \varnothing_1' \| \varnothing_1' \| \varnothing_1' \| X \| Z \| q_j)$. If $Ak\prime = Ak$, then the acceptor key of the patient is accepted by the doctor, else rejected.

Proof of correctness

$$
\begin{aligned}
T_1' &= \wp_{i\,d} \times X \\
&= g_x^{t+y_1+y_2} \times g_x^{-(y_1+y_2)} = g_x^{t} = T_1 \\
S_1' &= Y \times Z \\
&= g_x^{s+y_1-y_2} \times g_x^{y_2-y_1} = g_x^{s} = S_1 \\
\varnothing_1' &= R_1^{\varnothing_0-\partial_2-\partial_3} \\
&= R_1^{\mu_1+2\theta_j-(\theta_j-\mu_3)-\theta_j+\mu_4} \\
&= R_1^{\mu_3+\mu_4}.S_1^{\mu_1+\mu_2-\mu_4} \\
\varnothing_1' &= \frac{R_1^{\varnothing_0-\partial_2-\partial_3}.S_1^{\partial_3-\partial_1}}{T_1^{\partial_3-\partial_2}} \\
&= \frac{R_1^{\mu_1+2\theta_j-(\theta_j-\mu_3)-(\theta_j+\mu_4)}.S_1^{\theta_j+\mu_4-(\theta_j-\mu_2)}}{T_1^{\theta_j+\mu_4-(\theta_j-\mu_3)}} \\
&= \frac{R_1^{\mu_1+\mu_3-\mu_4}.S_1^{\mu_2+\mu_4}}{T_1^{\mu_3+\mu_4}} \\
&= \varnothing_3.
\end{aligned}
\tag{1}
$$

4.7. Patient's Signature Verification. If $e(\mathrm{sig}_{pa}, q_j .g_y^{H(DI_{pa})}) = e(g_x, g_y)$, then the message is accepted by the doctor and the doctor considers the patient as the authenticated patient. After confirming the patient, the doctor performs the diagnosis for the patient.

Proof of correctness

$$
\begin{aligned}
e\left(\mathrm{sig}_{pa}, q_j.g_y^{H(DI_{pa})}\right) &= e\left(\mathrm{sig}_{pa}, g_y^{\theta_j}.g_y^{H(DI_{pa})}\right) \\
&= e\left(g_x^{1/H(DI_{pa})+\theta_j}, g_y^{\theta_j+H(DI_{pa})}\right) \\
&= e\left(g_x, g_y\right).
\end{aligned}
\tag{2}
$$

Only if the signature and certificate are verified by the doctor, the patient is considered as the authenticated user and the doctor can get the required biotic statistics (BS) from the patient. If any one of the verification processes fails, then the patient is considered as an illegal user.

4.8. Doctor's Authentication. Here, the patient checks the authenticity of the doctor. Before sending the BS to the doctor, the patient should anonymously authenticate the doctor. Therefore, the doctor generates an anonymous competitor key as $Co_D = H\ (e(g_x, g_x)\|DI_D\|PU_D)$ and generates the certificate as $\mathrm{cer}_D = (DI_D\|PU_D\|TS\|\ A_D)$. The competitor key and certificate are sent to the patient's data sensor regulator. Initially, the TS value is checked by the patient. If the timing value is acceptable, then the patient's data sensor regulator checks $e(DI_D.A_D, A_1) = e(g_x, g_x)$.

Proof of correctness

$$
\begin{aligned}
e(DI_D.A_D, A_1) &= e\left(g_x^{s+d_i}.g_x^{t-d_i}, g_x^{1/s+t}\right) \\
&= e\left(g_x^{s+t}, g_x^{1/s+t}\right) \\
&= e(g_x, g_x).
\end{aligned}
\tag{3}
$$

Then the patient's data sensor regulator calculates the patient competitor key as $Co_{pa} = H(e(DI_D.A_D, A_1)\ \|DI_D\|PU_D)$. If $Co_{pa} = Co_D$, then the patient considers the doctor as the legitimate user and send his/her biotic statistics.

4.9. Confidentiality. To maintain confidentiality, the medical prescription (MP) of the doctor and the biotic statistics (BS) of the patient are encrypted using elliptic curve cryptography (ECC) encryption algorithm.

4.9.1. Encryption by the Patient. Initially a random number is chosen by the patient as l_i and the patient computes the cipher text as $CI_{pa} = (BS\|PU_{pa}\|T_{pa}) \oplus H(e(g_y, g_y)^{l_i})$. Therefore, the decrypted message can be calculated as $(BS\|PU_{pa}\|T_{pa}) = CI_{pa} \oplus H(e(g_y, g_y)^{l_i})$.

4.9.2. Decryption by the Doctor. Once the cipher text is received by the doctor, he performs the decryption operation as $CI_{pa} \oplus H(e(PU_D, \propto^{l_i}) = (BS\|PU_{pa}\|T_{pa})$.

Proof of correctness

$$
\begin{aligned}
H\left(e\left(PU_D, \propto^{l_i}\right) &= H\left(e\left(g_y^{d_i}, \left(g_y^{1/d_i}\right)\right)^{l_i}\right) \\
&= H\left(e\left(g_y, g_y^{l_i}\right)\right) \\
&= H\left(e\left(g_y, g_y\right)^{l_i}\right).
\end{aligned}
\tag{4}
$$

4.9.3. Encryption by the Doctor. Similarly, the medical prescription (MP) of the doctor should be sent in an encrypted way. Initially a random number is chosen by the doctor as l_j and he computes the cipher text as $CI_D = (MP\|PU_D\|T_D) \oplus H(e(g_x, g_x)^{l_j})$. The decrypted message can be calculated as $(MP\|PU_D\|T_D)\ CI_D = \oplus H(e(g_x, g_x)^{l_j})$.

4.9.4. Decryption by the Patient. Once the cipher text is received by the patient, he performs the decryption operation as $CI_D \oplus H(e(PU_{pa}, \beta^{l_j}) = (MP \| PU_D \| T_D)$.

Proof of correctness

$$\begin{aligned} H\left(e\left(PU_{pa}, \beta^{l_j}\right) &= He\left(\left(g_x^{a_i}, \left(g_x^{1/a_i}\right)^{l_j}\right)\right. \\ &= H\left(e\left(g_x, g_x^{l_j}\right)\right) \\ &= H\left(e\left(g_x, g_x\right)^{l_j}\right). \end{aligned} \tag{5}$$

4.10. Transfer Authentication. In the current scenario, when the patient moves from one doctor to another doctor in another region for medical diagnosis, the new doctor in another region needs to authenticate the patient once again. But in the proposed scheme, transfer authentication is performed between the previous doctor and the current doctor. The previous doctor sends the IC of the particular patient to the current doctor. If the $IC \neq 0$, then the corresponding patient is considered as the authenticated patient and he will be accepted to get the service from the current doctor. Moreover, if $IC \neq 0$ then the previous doctor provides the BS of the corresponding patient and other required information. Hence, it is not required for the current doctor to authenticate the IC again. The following steps are executed as follows.

(1) The previous doctor chooses a random number $x \in Z_q^*$ and generates two transfer keys TK_1 and TK_2, where $TK_1 = S_{D,1}^{xH(DI_p \| IC)}$ and $TK_2 = PU_{D+1}^{xd_i}$. These transfer keys are sent to the current doctor. Moreover, $PU_D = g_y^{d_i}$ and $PU_{D+1} = g_y^{d_i+1}$ represent the public key of the previous and current doctor, respectively. Moreover, the transfer key TK_2 is sent to the particular patient.

(2) Then the current doctor picks a random number $c \in Z_q^*$ as its private key and computes the transfer keys as $TK_D = g_x^c$ and $TK_{D,1} = g_y^c$. Here, TK_D is kept as secret by the current doctor and $TK_{D,1}$ is given to the particular patient.

(3) Moreover, the current doctor generates the session transfer keys as $TK_\beta = TK_1^{d_{i+1}}$ and $TK_{\beta,1} = TK_\beta . TK_D$. Here, $d_{i+1} \in Z_q^*$ is the private key of the current doctor. The current doctor generates the new session key as $SN_D = e(g_y, TK_{\beta,1})$.

(4) Hence, by receiving the transfer keys TK_2 and $TK_{D,1}$ from the previous and current doctor, the patient computes the patient's transfer keys as $TK_{pa} = TK_2^{d_i . H(DI_p \| IC)}$ and $TK_{pa,1} = TK_{pa} . TK_{D,1}$, respectively.

(5) Finally, the patient calculates the patient's new session key.

(6) $SN_{pa} = e(TK_{pa,1}, g_x)$. If $SN_D = SN_{pa}$, then the current doctor accepts the particular patient's data and the transfer authentication task is accomplished.

Proof of correctness

$$\begin{aligned} SN_D &= e\left(g_y, TK_{\beta,1}\right), \\ &= e\left(g_y, TK_\beta . TK_D\right) \\ &= e\left(g_y, TK_1^{d_{i+1}} . TK_D\right) \\ &= e\left(g_y, S_{D,1}^{d_{i+1} . xH\left(DI_p \| IC\right)} . g_x^c\right) \\ &= e\left(g_y, g_x^{d_{i.} a_{i.} d_{i+1} . xH\left(DI_p \| IC\right)} . g_x^c\right) \\ &= e\left(g_x, g_y^{d_{i.} a_{i.} d_{i+1} . xH\left(DI_p \| IC\right)} . g_y^c\right) \\ &= e\left(g_x, TK_2^{a_{i.} H\left(DI_p \| IC\right)} . TK_{D,1}\right) \\ &= e\left(g_x, TK_{pa} . TK_{D,1}\right) \\ &= e\left(g_x, TK_{pa,1}\right) \\ &= SN_{pa}. \end{aligned} \tag{6}$$

5. Security Analysis

The various possible security attacks and the security features provided by the suggested scheme are explained in this section.

5.1. Resistance to Impersonation Attack. In order to perform impersonation attack and to find the secret parameters of the authorized doctor/patient, the attacker should pretend to act like an authorized doctor/patient. The certificate for the patient is calculated as $\text{cer}_{pa} = (\wp_{i\ d} \| Ak \| q_j \| \varnothing_0 \| \partial_1 \| \partial_2 \| \| \partial_3 \| \| X \| Y \| Z)$. To find the values of X, Y, and Z, the randomly chosen numbers y_1, y_2 and the secret key of MN such as s should be known by the adversary. Since the numbers y_1 and y_2 are random, the values of X, Y, and Z are also random which is difficult to find due to ECDLP and the secret key of MN is also difficult to find by an adversary. Similarly, the certificate of the doctor is calculated as $\text{cer}_d =((DI_D \| PU_D \| TS \| A_D)$. Here, A_D is calculated from the doctor's private key and MN private key, where $A_D = g_x^{t-d_i}$. Since the private keys are secret and are known only to MN, it is difficult for an intruder to find the values of A_D and to forge the certificate. Moreover, a unique identity code is generated by MN for each authorized patient and it is stored in the blockchain network. Any change in the identity code will be reflected in the succeeding blocks in the blockchain. So, the miners in the network will remove the particular unauthenticated patient (adversary) from the network.

5.2. Resistance to Fake Message Attack. To send fake message, adversary should create a bogus message similar to the original real message as $\text{mess}_{pa} = (DI_D \| q_j \| yy \| \text{sig}_{pa})$. Here DI_{pa} is calculated from the secret keys of MN and patient, so it is difficult for an adversary to find the value of DI_{pa}. Moreover, the value of yy involves X, Y, and Z. As the values of X, Y, and Z are calculated based on the random numbers y_1 and y_2, it is difficult to find yy due to ECDLP. To find the values of y_1 and y_2 , there is a complexity of $O[f^{1/2+o(1)}\log \omega]$ where 'ω' represents number of patients registered in the network.

5.3. Resistance to Message Alteration Attack. To perform message alteration/modification attack, the adversary should decrypt the data sent by the authenticated doctor or the authenticated patient. In order to perform the decryption operation, the adversary should have a knowledge regarding the decryption keys of patient/doctor. But these decryption keys $(\propto, \beta)$ are provided by the MN during the initial offline registration of doctor and patient in a secure way. Moreover, to calculate the decryption keys, the private key of the doctor (d_i) and the private key of the patient (a_i) provided by the MN should be known to the adversary. In addition, during the authentication process, signature is generated as $\mathrm{sig}_{pa} = g_x^{1/H(DI_{pa})+\theta_j}$, which involves short-life private key θ_j and dummy identity DI_{pa} of the patient which are hard to trace. Hence, it is difficult for an adversary to undergo message alteration attack.

5.4. Conditional Privacy Preservation. In this proposed scheme, the doctor and the patient use anonymous certificate and signature to hide their real original identity. Only the dummy identity of the end-user is used during the mutual authentication process. So, even though the adversary finds the dummy identity of the end-users, it is a challenging phenomenon for an adversary to trace the real identity. Moreover, if the end-users are compromised, then by using the tracking list, the MN revokes the compromised end-users from the network. Thus in this proposed scheme, conditional privacy is preserved.

5.5. Resistance to Repudiation Attack. In this suggested scheme, the end-users cannot repudiate once the information is received. Here, the doctor sends the MP to the authenticated patient and the patient sends the BS to the authenticated doctor. The MP is sent in the form of cipher text $CI_D = (MP \| PU_D \| T_D) \oplus H(e(g_x, g_x)^{l_j})$ by including the tracking parameter. So, in case of any dispute due to wrong prescription of the doctor, the MN can track the doctor from the doctor's tracking parameter list. Similarly, the BS of the patient is sent in the form of cipher text $CI_{pa} = (BS \| PU_D \| T_{pa}) \oplus H(e(g_y, g_y)^{l_j})$ to the doctor. So, if any wrong information/data is sent by the patient, then the MN can easily track the patient based on the patient's tracking parameter list. So, the end-users cannot repudiate.

5.6. Resistance to Reply Attack. In the reply attack, the adversary wants to capture the message within a specific time interval, modify/create the message, and send it to the end-users. But in the proposed scheme, timestamps (TS) are attached to the anonymous message. Due to the presence of the TS, the adversary cannot perform the message modification/creation in the given stipulated time. Thus, the proposed scheme is resistant to reply attack.

5.7. Unlinkability. The data sensor regulator of the patient selects $q_j = g_y^{\theta_j}$ as the short time public key, where θ_j is the short time private key such that $\theta_j \in Z_p^*$ and $j < p$. Short-life private keys are used for the certificate and signature generation. The validity of these private keys is only for a short duration. So, once the verification process is completed, the validity of these keys get expired. Therefore, there is an unlinkability existing in the generation of the certificates. Hence, an adversary cannot link the two certificates generated by the same end-users.

5.8. Man-in-Middle Attack. The proposed work is resistant to man-in-middle (MM) attack. During the exchange of information, the patient sends their biotic statistics (BS) to the doctor in the form of cipher text by including the timestamp. Similarly, the doctor sends the medical prescription (MP) in an encrypted way by attaching the timestamp. In our work, if the intruder tries to capture the BS/MP, only a zero knowledge is obtained from the exchanged data. Moreover, if the intruder sends the new fake data in place of original data, because of the presence of timestamp, the data will be received with a delay and hence it is not accepted. Hence MM attack is not possible.

6. Performance Analysis

The performance analysis of the suggested scheme is analyzed in terms of computational complexity and communication cost.

6.1. Computational Complexity. Computational complexity of the proposed scheme is compared with the relative existing schemes like Liu et al. [29], Zhao [30], Hu et al., [31] and Al-Riyami and Paterson [32]. Computational complexity is analyzed in terms of cryptographic functions like T_m, T_h, T_e, and T_p. Here, T_m, T_h, T_e, and T_p are the representations used for one point multiplication, one point hash function, exponential function, and bilinear pairing operation. Moreover, cryptographic operations are implemented with core i7 processor having 8 GB RAM using PBC library [33]. In addition, the platform used for the execution process is Cygwin [34]. The time required for the execution of T_m, T_h, T_e, and T_p is 0.7 ms, 2.6 ms, 0.6 ms, and 1.72 ms, respectively. Here 'ms' represents milliseconds. Table 2 shows the computational cost for different schemes in terms of certificate and verification cost. Generally the time required for the hashing operation and pairing operation is higher when compared to other operations. In our suggested scheme, only two pairing operations and one hashing operation are required for verifying the signature and certificate of single patient/doctor, whereas Liu et al. [29] scheme requires three pairing and three hashing operations. Zhao [30] scheme requires three pairing and eleven hashing operations. Hu et al. [31] scheme requires four pairing and

Table 2: Computational cost for different schemes.

Schemes	Verification cost for single certificate and single signature	Verification cost for n certificates and n signatures
Liu et al.	$3T_p + 3T_h + 3T_m$	$3nT_p + 3nT_h + 3nT_m$
Zhao et al.	$9T_m + 11T_h + 3T_p$	$9nT_m + 11nT_h + 3nT_p$
Hu et al.	$2T_m + 6T_h + 4T_p$	$(n+1)T_m + 6nT_h + 4nT_p$
Riyami et al.	$T_h + 4T_p + T_e + T_m$	$nT_h + 4nT_p + nT_e + nT_m$
Proposed (patient)	$\mathbf{2T_p + T_h + T_m + 2T_e}$	$\mathbf{(n+1)T_p + nT_h + nT_m + 2nT_e}$
Proposed (doctor)	$\mathbf{2T_p + T_h}$	$\mathbf{(n+1)T_p + nT_h}$

six hashing operations. Similarly, Al-Riyami and Paterson [32] scheme require four pairing operations and one hashing operation. The suggested scheme consumes less computational cost when compared to the existing related schemes. The verification cost for the single patient is 12.12 ms and the verification cost for the single doctor is 6.02 ms whereas the related schemes like [29–32] take 15.03 ms, 23.84 ms, 40.03 ms, and 12.84 ms, respectively. Verification cost for single certificate and single signature in the suggested work for the patient and the doctor patient is

$2T_p + T_h + T_m + 2T_e$ and $2T_p + T_h$, respectively. In a nutshell, only two pairing functions and one hashing function required verifying a single certificate and single signature. If n number of end-users is taken into consideration, proposed work consumes $(n+1)T_p$ pairing and nT_h hashing operation.

The graphical representation of the computational cost for the different schemes with respect to patients and doctors is shown in Figures 3 and 4, respectively. It is clearly observed that the proposed scheme consumes only 209.91 ms and 38.51 ms for the verification of 20 certificates and 20 signatures for the patients and doctors, respectively. As a result, within the stipulated time, proposed scheme can verify the certificate and signature significantly. The verification cost for the existing related schemes is higher than 260 ms for the verification of signature and certificate for the same number of end-users. Thus the verification cost is very low when compared to the related existing works.

6.2. Communication Cost. The communication cost of the proposed work is compared with existing works, namely, Liu et al. [29], Zhao [30], Hu et al. [31], and Al-Riyami and Paterson [32]. This section deals with the cost incurred during the exchange of information between the doctors and patients. As per Liu et al. [29] scheme, the number of bits required for single message is 3840 bits. Zhao [30] scheme requires 2112 bits for transferring a single message. Hu [31] and Al-Riyami and Paterson [32] schemes require 2496 bits and 1536 bits, respectively. Thus when compared to the existing schemes, the suggested scheme consumes less communication cost which improves the efficiency of the proposed scheme. In this work, type A elliptic curve is used for the calculation of the communication cost. Table 3 shows the communication cost for different schemes. The bit size for the parameters used in the groups G_x, G_y, and G_z is 160 bits. Moreover, the bit size of the elements belonging to Z_q^* is 160 bits, time stamp's bit size is 32 bits, and the bit size of hash function's output is 160 bits. In the proposed scheme,

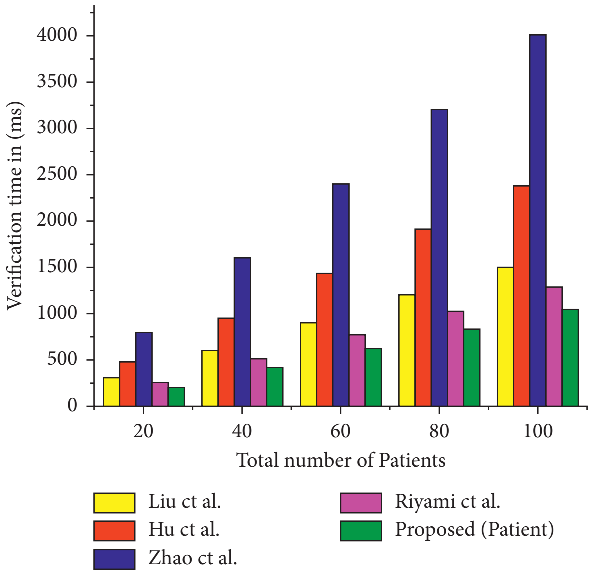

Figure 3: Computational cost for different schemes with respect to patients.

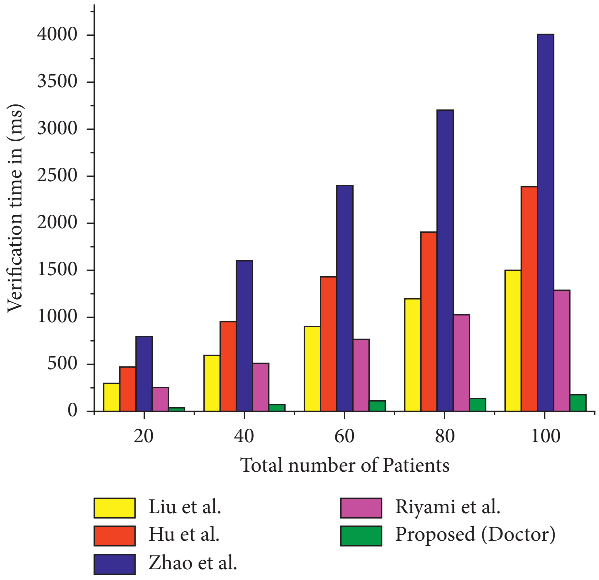

Figure 4: Computational cost for different schemes with respect to doctors.

the cipher text for the patient and the doctor is calculated as $CI_{pa} = (BS\|PU_D\|T_{pa})\oplus H(e(g_y, g_y)^{l_j})$ and $CI_D = (MP\|PU_D\|T_D)\oplus H(e(g_x, g_x)^{l_j})$. Moreover, time stamp is used

Table 3: Communication cost for different schemes.

Schemes	Number of bits for single message	Number of bits for n messages
Liu et al.	3840	3840 n
Zhao et al.	2112	2112 n
Hu et al.	2496	2496 n
Riyami et al.	1536	1536 n
Proposed scheme	**1344**	**1344 n**

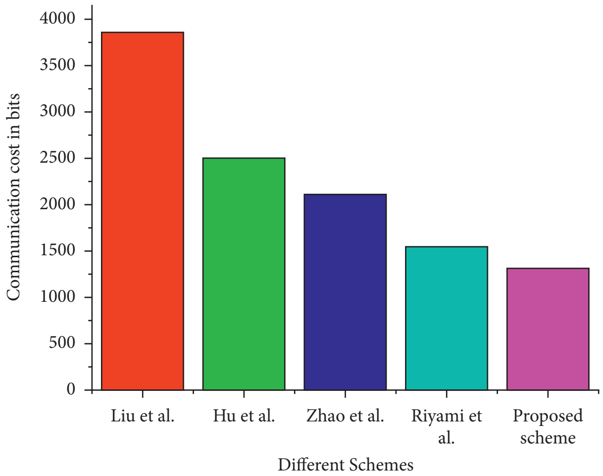

Figure 5: Communication cost for different schemes.

during the mutual authentication between the doctor and patient and it consumes 64 bits. MP and BS are the elements belonging to Z_q^* and they totally consume 320 bits. PU_{pa}, T_{pa}, PU_D, and T_D are the elements in the groups and they totally consume 640 bits. The output of the two hash functions consumes 320 bits. So totally, 1344 bits are required as the communication cost for the proposed scheme. Figure 5 shows the pictorial representation of the communication cost for different schemes. From Figure 5, it is clear that the proposed work consumes less bit size when compared to the related works.

7. Conclusion

In this work, an efficient blockchain-based lightweight mutual anonymous authentication protocol for the end-users (patients and doctors) is proposed. The proposed work can be practically deployed between the patients and doctors in hospitals. Here, the encryption of both BS data of the patient and the confidential MP of the doctor is performed to preserve confidentiality. Only the authenticated end-user can decrypt the data. In addition, the certificate and signature verification signifies the message's integrity. Moreover, the suggested scheme can withstand several security threats. Further, transfer authentication protocol helps to avoid the reauthentication of the patient again, when they move to the new doctor which reduces the communication and computational cost significantly. Since blockchain is used, there is a continuous tracking of data, as they are stored in the distributed ledger. As a result, there is no tampering/modification of data. Thus, the proposed scheme can be effectively deployed in the hospitals for monitoring the patient's data.

The main advantage of the proposed scheme is to preserve the confidentiality, integrity, and security of the transferred data. However, the scheme is limited to the inclusion of biometric authentication. Future work direction can be extended to cloud-assisted blockchain-based schemes to enhance the storage of large volumes of confidential information, not only enhancing the data storage by using the cloud-assisted blockchain, but also enhancing the monitoring process of the patient's data. Moreover, fine tuning method can be incorporated to enhance the data quality. Furthermore, high-level requirements are down-converted into low level requirements for the doctors to improve the efficiency.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1658–1686, 2014.

[2] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," *Future Generation Computer Systems*, vol. 78, pp. 956–963, 2018.

[3] V. Odelu, S. Saha, R. Prasath, L. Sadineni, M. Conti, and M. Jo, "Efficient privacy preserving device authentication in WBANs for industrial e-health applications," *Computers & Security*, vol. 83, pp. 300–312, 2019.

[4] A. Abuelkhail, U. Baroudi, M. Raad, and T. Sheltami, "Internet of things for healthcare monitoring applications based on RFID clustering scheme," *Wireless Networks*, vol. 27, no. 1, pp. 747–763, 2020.

[5] A. Arasan, R. Sadaiyandi, F. Al-Turjman, A. S. Rajasekaran, and K. Selvi Karuppuswamy, "Computationally efficient and secure anonymous authentication scheme for cloud users," *Personal and Ubiquitous Computing*, vol. 25, 2021.

[6] J. S, M. Azees, A. Sekar, and F. Al-Turjman, "Lightweight privacy and confidentiality preserving anonymous authentication scheme for WBANs," *IEEE Transactions on Industrial Informatics*, p. 1, 2021.

[7] J. Subramani, A. Maria, R. B. Neelakandan, and A. S. Rajasekaran, "Efficient anonymous authentication

scheme for automatic dependent surveillance-broadcast system with batch verification," *IET Communications*, vol. 15, no. 9, pp. 1187–1197, 2021.

[8] M. Azees, P. Vijayakumar, M. Karuppiah, and A. Nayyar, "An efficient anonymous authentication and confidentiality preservation schemes for secure communications in wireless body area networks," *Wireless Networks*, vol. 27, no. 3, pp. 2119–2130, 2021.

[9] A. Iqbal, A. S. Rajasekaran, G. S. Nikhil, and M. Azees, "A secure and decentralized blockchain based EV energy trading model using smart contract in V2G network," *IEEE Access*, vol. 9, pp. 75761–75777, 2021.

[10] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wirelessbody area networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 332–342, 2014.

[11] M. H. Ibrahim, S. Kumari, A. K. Das, M. Wazid, and V. Odelu, "Secure anonymous mutual authentication for star two-tier wireless body area networks," *Computer Methods and Programs in Biomedicine*, vol. 135, pp. 37–50, 2016.

[12] H. Zhao, P. Bai, Y. Peng, and R. Xu, "Efficient key management scheme for health blockchain," *CAAI Transactions on Intelligence Technology*, vol. 3, no. 2, pp. 114–118, 2016.

[13] H. Debiao, S. Zeadally, N. Kumar, and J. H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2590–2601, 2017.

[14] 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, pp. 429–443, 2017.

[15] X. Li, J. Peng, F. Wu, M. Karuppiah, and K.-K. Raymond Choo, "An enhanced 1-round authentication protocol for wireless body area networks with user anonymity," *Computers & Electrical Engineering*, vol. 61, pp. 238–249, 2017.

[16] E. Luo, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu, and M. Atiquzzaman, "PrivacyProtector: privacy-protected patient data collection in IoT-based healthcare systems," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 163–168, 2018.

[17] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," *Journal of Network and Computer Applications*, vol. 106, no. 6, pp. 117–123, 2018.

[18] C.-T. Li, C.-C. Lee, C.-Y. Weng, and C.-M. Chen, "Towards secure authenticating of cache in the reader for RFID-based IoT systems, Peer-to-Peer Netw," *Apple*, vol. 11, no. 1, pp. 198–208, 2018.

[19] D. Deebak, F. Al-Turjman, and L. Mostarda, "A hash-based RFID authentication mechanism for context-aware management in IoT-based multimedia systems," *Sensors*, vol. 19, no. 18, p. E3821, 2019.

[20] B. A. Alzahrani, A. Irshad, A. Albeshri, K. Alsubhi, and M. Shafiq, "An improved lightweight Authentication protocol for wireless body area networks," *IEEE Access*, vol. 8, pp. 190855–190872, 2020.

[21] T. Jabeen, H. Ashraf, A. Khatoon, S. S. Band, and A. Mosavi, "A lightweight genetic based algorithm for data security in wireless body area networks," *IEEE Access*, vol. 8, pp. 183460–183469, 2020.

[22] Z. U. Rehman, S. Altaf, and S. Iqbal, "An efficient lightweight key agreement and authentication scheme for WBAN," *IEEE Access*, vol. 8, pp. 175385–175397, 2020.

[23] O. Amjad, E. Bedeer, N. Abu Ali, and S. Ikki, "Robust energy efficiency optimization algorithm for health monitoring system with wireless body area networks," *IEEE Communications Letters*, vol. 24, no. 5, pp. 1142–1145, 2020.

[24] A. Kumar, K. Singh, T. Khan, A. Ahmadian, M. H. M. Saad, and M. Manjul, "ETAS: an efficient trust assessment scheme for BANs," *IEEE Access*, vol. 9, pp. 83214–83233, 2021.

[25] E. Lara, L. Aguilar, and J. A. Garcia, "Lightweight Authentication protocol using self-certified public keys for wireless body area networks in health-care applications," *IEEE Access*, vol. 9, pp. 79196–79213, 2021.

[26] Z. Ning, "Mobile edge computing enabled 5G health monitoring for internet of medical things: a decentralized game theoretic approach," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 463–478, 2021.

[27] 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.

[28] C. Guo, P. Tian, and K.-K. R. Choo, "Enabling privacy-assured fog-based data aggregation in E-healthcare systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 1948–1957, 2021.

[29] J. Liu, L. Zhang, and R. Sun, "1-raap: an efficient 1-round anonymous authentication protocol for wireless body area networks," *Sensors*, vol. 16, no. 5, p. 728, 2016.

[30] Z. Zhao, "``An ef_cient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem," *Journal of Medical Systems*, vol. 38, no. 2, 2014.

[31] C. Hu, H. Li, Y. Huo, T. Xiang, and Z. Liao, "Secure and efficient data communication protocol for wireless body area networks," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 2, no. 2, pp. 94–107, 2016.

[32] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology_ASIACRYPT (Lecture Notes in Computer Science)*Springer-Verlag, New York, NY, USA, 2003.

[33] Pbc library, "Tech. rep.," 2019, http://crypto.standford.edu/pbc/.

[34] Cygwin, https://www.cygwin.com/, 2019.