Blockchain-based Data Access Security Solutions for Medical Wearables

Hui Lin, Quanwen He, Jia Hu, and Xiaoding Wang*

***Abstract*—Digital healthcare services have become an integral part of our lives. There is an increasing number of healthcare professionals and patients using medical wearables for diagnosis and treatment, which simplifies and improves the diagnostic and therapeutic process. However, inappropriate use of medical data may result in the disclosure of private patient information. For protecting patients' privacy when using medical wearables, we propose a new blockchain-based data access security scheme. Specifically, the elliptic curve encryption algorithm and zero-knowledge authentication method are used to authenticate the identity of patients and doctors in the blockchain network. Furthermore, we develop a smart recommendation method based on deep reinforcement learning to recommend appropriate doctors for patients. Next, patients allow recommended doctors to access their medical data, and smart contracts specifically designed for secure data access to medical wearables will regulate subsequent data access. The security analysis and experimental results demonstrate that the proposed scheme can effectively protect patients' privacy during treatment through secure authentication and data access for medical wearables.**

***Index Terms*—Medical Wearables, Blockchain, Machine Learning, Privacy Protection, Data Access.**

I. Introduction

Since January 2020, the COVID-19 pandemic has swept across the world, and many countries are facing a critical situation with a dramatic increase in the number of patients, many of whom have difficulty accessing care from primary doctors or caregivers [1]. In recent years, the Internet of Things (IoT) and wearable devices have flourished, using which the remote patient monitoring and data analysis can improve the quality of medical care [2]. With the deployment of 5G technology, one of the key IoT applications is wearable device networks, which collects patients' test data such as blood pressure, heart rate and blood sugar levels through medical wearables, and transmits patients' health data to doctors through smart devices such as smartphones and tablets for health monitoring, diagnosis and treatment of diseases [3], [4].

In order to jointly process patient monitoring data in medical institutions at all levels, secure data sharing is required among wearable devices. However, patients' medical data is highly confidential, and sharing data may result in the disclosure of patients' personal information and health data [5]. Moreover, the patients' data should be owned by themselves, so they have the right to manage their medical data, and the doctors can access the relevant data only after being authorized by the patients [6]. However, due to the limitation of network infrastructure, the existing medical system is inadequate to support the safe sharing of medical data. For example, most current IoT data sharing models are based on centralized architectures, in which if the data center is attacked, the entire system will be out of service and data will be compromised. In addition, medical systems are vulnerable to privacy breaches due to illegal access [7]. According to Comparitech's statistics, from 2009 to 2022, the medical institutions in the United States suffered nearly 5000 data leakage incidents, affecting more than 342 million medical records. Among them, 2020 is the year with the largest number of medical data leakage incidents, with a total of 803. The number of data leakage incidents in 2021 was also very high, reaching 711, followed by 520 in 2019. This shows that medical data leakage incidents have increased exponentially in the past three full years.

The above analysis suggests that data sharing in medical wearable devices should first address the problem of access control. Access control technology is one of the cornerstones of data protection, which is used to control the data security interaction between access subjects and objects. At present, the main access control models include role-based access control (RBAC) [8], attribute-based access control (ABAC) [9] and task-based access control (TBAC) [10]. These access control models have defects in maintaining data's ownership and defining access rights, and there are problems of single access control and centralized policy decisions, which makes the access control mechanism itself unreliable. Besides, selecting a third party to centrally organize the implementation of access control management will lead to many security regulatory loopholes, face multiple threats such as internal illegal operations and external illegal attacks, and is not easy to track and verify. If these access control models are used in the data sharing of medical wearable devices, it will inevitably lead to misdiagnosis, thus making patients unable to receive timely treatment. Therefore, in order to enhance the security of wearable medical devices and protect the privacy of patient data, it is necessary to design a reliable and efficient identity authentication and data access control mechanism [11].

The access control mechanism based on smart contracts allows users to use smart contracts to control the access to all data interaction processes between the subject and object, and realize the supervision and management of all data such as the attribute status of the subject and object, the authorization

Hui Lin, Quanwen He, and Xiaoding Wang (Corresponding author *) are with the College of Computer and Cyber Security, Fujian Normal University, Engineering Research Center of Cyber Security and Education Informatization, Fujian Province University, Fuzhou, Fujian, 350117, China, e-mails: linhui@fjnu.edu.cn, heqw15890514263@163.com, and wangdin1982@fjnu.edu.cn.

Jia Hu is with the University of Exeter, EX4 4RN Exeter, U.K., e-mail: j.hu@exeter.ac.uk.

traceability information, the policy update history, and so on [12]. In a decentralized, tamper proof and traceable network environment of blockchain, medical data can be encrypted and stored on the blockchain. By setting access permissions through smart contracts, users can achieve efficient and secure point-to-point data sharing. In addition, the execution status and result data of the smart contract will be recorded on the blockchain in the form of transactions and cannot be revoked [13] such that the data reliability is fully guaranteed. This means the authentication and access control based on smart contracts provide new solutions for medical data privacy protection. However, we still need to address the issue of how to intelligently and reasonably determine the identity and authority of patients and doctors in smart contracts, which poses a new challenge to the diagnosis supported by medical wearable devices.

To address this problem, we propose a new blockchain-based data access security scheme to protect patients' data privacy. The main contributions of this paper are summarized as follows:

1) To provide effective authentication, the elliptic curve encryption algorithm and zero-knowledge authentication method are used to authenticate the identity of patients and doctors in the blockchain network.
2) To provide better treatment, we develop a smart recommendation method based on deep reinforcement learning to recommend appropriate doctors for patients. Specifically, we use the average match between the patients' diseases and the doctors' expertises to design a doctor recommendation mechanism based on the deep reinforcement learning algorithm DQN to ensure that all patients can be recommended to the appropriate doctors.
3) To realize efficient access control, the patients grant the recommended doctors the access to their medical data, following a procedure which is monitored and guided by the smart contract specifically designed for secure data access of medical wearables.
4) The security analysis and experimental results demonstrate that the proposed scheme can effectively protect patients' privacy during treatment through secure authentication and data access for medical wearables.

We organize the rest of this paper as follows. The related works are covered in Section II. The background knowledge is introduced in Section III. The system model is presented in Section IV. The implementation details of the proposed scheme is given in Section V. The security analysis is provided in Section VI. The performance evaluation is conducted in Section VII. This paper is concluded in Section VIII.

II. Related Work

The research on secure data access in the medical industry has received extensive attention from scholars, and a large number of related research work has been published. The work related to secure data access falls within three categories, namely, public key based, smart contract based, and machine learning based.

Public Key based Data Access. Axon *et al.* [15] showed that blockchains can be used to build a privacy aware PKI, while eliminating some of the problems encountered in traditional PKIs. Then, they proposed PB-PKI [16], a privacy-aware framework, which stores the key under the chain and encrypts the key on the chain to avoid binding user identity and public key, thus protecting identity privacy. The framework divides user identity privacy into global privacy and adjacent local privacy.In the neighborhood trusted node, the user identity is bound to the public key. In the globally untrusted nodes, the offline key is used to protect identity privacy. Ali *et al.* [17] proposed Blockstack, which is a large-scale deployed distributed PKI system built on a blockchain system. Bui *et al.* [18] proposed that in distributed group member management, entities are represented by public keys, authorization information is encoded into the signature certificate, and then the hash value of the revocation certificate is stored on the blockchain. Although these identity authentication schemes can effectively solve the problems of single point of failure and certificate transparency, the cost of computing resources in the management and maintenance of public key certificates is huge.

Smart Contract based Data Access. Aiming at the characteristics of high difficulty in medical data management, complex data subjects, and incomplete privacy protection, MedRec [19], [20] used smart contracts to achieve access control of medical data on the blockchain, and adopts distributed data integration and access control for medical data of different departments and levels. MedRec has three levels of contract. Registration contracts are used to manage patient identity information, authorization contracts are used to achieve data permission management, and associated contracts SC bind patient identity information and corresponding role permissions. Guo *et al.* [21] proposed a hybrid blockchain-edge architecture. This architecture combines the technology of blockchain and edge intelligence to realize the access control management of electronic health records via smart contracts. Song *et al.* [22] designed an attribute-based access control using smart contracts scheme for IoT. This scheme solved the dynamic, distributed and reliable access control problems in an open IoT environment. Sultana *et al.* [23] proposed a data sharing and access control system, which is used for communication between devices in the IoT. The system provides effective access control management through access control contract, registration contract and judgment contract, and realizes the authentication of data sharing. Authentication and access control based on smart contracts provide ideas for the protection of medical data privacy, but the problem of reasonably setting the identity and authority of patients and doctors in smart contracts still needs to be solved, especially in the field of diagnosis supported by medical wearables.

Machine Learning based Data Access. Liu *et al.* [24] proposed an efficient permission decision scheme based on machine learning, which converted attribute based access control requests into permission decision vectors, and converted the access control permission decision problem into a binary classification problem. Tay *et al.* [25] combined machine learning and dynamic authorization technology to adaptively adjust the role and policy control for intelligent performance perception. According to the user's performance, the new

roles and authorization levels are systematically updated with respect to the system constraints. Esposito *et al.* [26] proposed a novel identity and authorization policy distributed management solution by leveraging blockchain technology. Fragkos et al. [27] proposed a new hybrid role access control model based on the principles of offline deep reinforcement learning and Bayesian belief networks. This model utilizes a completely offline agent to model the user's behavior history as a trust index based on Bayesian beliefs, ensuring that internal users comply with system security rules, while dynamically improving the access control model through policy learning. Liu et al. [28] proposed a novel random access scheme for machine-type-communication devices, which maximized the access efficiency for contention-free and contention-based random access. Given the limited delay and set of random access opportunities, the random access control model is built to maximize random access efficiency. Lin et al. [29] proposd an attribute based security access control mechanism. This mechanism established the relationship between doctors' social attributes and their trusts, and combines graph convolutional networks with the SIR model based loss function to calculate doctors' trust. Doctors are only allowed to access specific medical data when their trusts are above the corresponding threshold. Despite the efficiency and intelligence in data access, these schemes have problems such as insufficient data privacy protection, insecure transmission process, and low sharing efficiency.

Different from the existing solutions, the proposed solution aims to provide a secure, intelligent and efficient data access solution to assist patients in treatment. To this end, we apply zero-knowledge proof and elliptic curve encryption to user authentication. In addition, we use machine learning to intelligently recommend online doctors based on patients' syndromes to achieve timely diagnosis. Moreover, we combine data access control with the design of smart contracts to protect the data privacy of patients.

III. Background

The authentication of user identity in medical wearable device system is designed based on elliptic curve algorithm and zero knowledge proof. To ensure the secure medical data sharing on the Ethereum platform, we use smart contracts to improve the efficiency and security of access control. For clarity, we first introduce three important technologies, namely the Ehtereum, the Elliptic Curve Encryption, and the Zero Knowledge Proof.

- Ehtereum [30]: Ethereum is an open source, global decentralized computing infrastructure that can be used to execute smart contracts. Developers can use the Turing complete programming language inside Ethereum to create decentralized applications with any consensus mechanism. Ethereum virtual machines run on miners, and transactions require miners to participate in repeated hashing to generate work. The cost of executing functions in smart contracts in Ethereum is GAS, which is generated by an Ethereum conversion. In general, Ethereum is the medium used to pay transaction fees and computing services on Ethereum, and gas consumed is used to reward miners.
- Elliptic Curve Cryptosystem (ECC) [31]: At present, the most commonly used identity authentication mechanisms are basically based on RSA algorithm. However, with the continuous improvement of security requirements in various fields, the length of keys used by RSA is also increasing, which directly leads to the increase of RSA computing. Compared with RSA, ECC requires much less keys and can achieve the same level of security. Its essence is a discrete logarithm problem on an elliptic curve. Suppose p is a prime number in a prime field modulo P, and $e_p(a,b)$ is a nonsingular elliptic curve in a prime field f_p. Then, $e_p(a,b)$ is represented by
$$y^2 = x^3 + ax + b, \tag{1}$$
where $x, y \in f_p$ and $4a^3 + 27b^2 \neq 0$.
- Zero Knowledge Proof [32]: The identity authentication technology based on zero-knowledge proof requires that the authenticator can prove that he/she is a legitimate user without letting the authenticator get any useful information during the authentication process, thus ensuring the security of the information. To be specific, Interactive zero-knowledge proof refers to the realization of interactive response in the connection process of the two parties executing the protocol. After the prover $\mathbf{P}$ executes the one-step protocol, the verifier $\mathbf{V}$ responds, and $\mathbf{P}$ responds accordingly according to the response of $\mathbf{V}$, repeating the process until the whole interaction is completed. The zero-knowledge proof of security needs to satisfy the following three properties, namely correctness, completeness and Zero knowledge. To be specific, for correctness, prover $\mathbf{P}$ cannot fool prover $\mathbf{V}$. In other words, if $\mathbf{P}$ doesn't know something, the probability that $\mathbf{V}$ believes $\mathbf{P}$ is low. For completeness, verifier $\mathbf{V}$ cannot deceive verifier $\mathbf{P}$, i.e., if $\mathbf{P}$ knows something, $\mathbf{P}$ can always convince the verifier. For zero knowledge, verifier $\mathbf{V}$ cannot obtain any information about knowledge during the verification process.

IV. System Model

In this paper, we consider a remote patient monitoring model based on blockchain as shown in Figure 1, which consits of the following objects, namely the data owner ($\mathbf{DO}$), the data user ($\mathbf{DU}$), the trusted authority ($\mathbf{TA}$), edge servers ($\mathbf{ES}$), intelligent devices, wearable devices, blockchain networks and distributed data storage systems.

- $\mathbf{TA}$: It generates registration information for users, which is verifiable. The successfully registered user will get the identity certificate generated by the trusted authority.
- $\mathbf{DO}$: It refers to the patient who provides health data. He/she needs to register with the trusted authority and obtain unique identity. The $\mathbf{DO}$ submits the health data through the intelligent terminal, encrypts the health data with the symmetric encryption algorithm, obtains the ciphertext, and sends it to the InterPlanetary File System (IPFS) outside the chain. Then, IPFS will return a download link to retrieve the data and store the key locally.

- **DU**: It refers to the doctor who requests for the **DO**'s health data.
- **ES**: It refers to an entity that can verify the identity of users and generate access credentials for data access. When the data access on the chain is abnormal, it can be traced back to the user's identity.
- Intelligent Devices: Smart IoT [33] terminals (such as mobile phones and computers) are devices used by patients to interact with blockchain networks.
- Wearable Devices: The devices (such as bracelets) collect health data of patients, including blood pressure, heart rate, blood glucose, blood lipid and sleep status.
- Blockchain Networks: It is responsible for both access control and data verification. Each user must access the health data through the access control on the blockchain. After successfully obtaining the data, the user can verify the consistency and integrity of the data through the blockchain.
- Distributed Data Storage Systems: In this paper, the IPFS is considered. The data is stored in IPFS after encryption. If the **DU** want to retrieve the data, he/she needs the authorization of the **DO** to obtain the data decryption key.

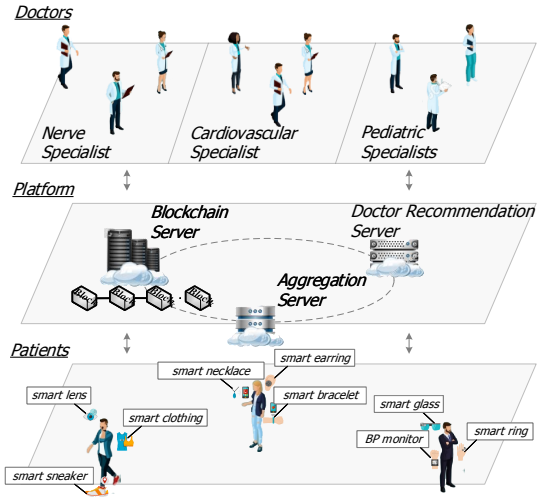


Fig. 1. Remote patient monitoring model.

In this model, patients send their own vital signs collected by medical wearables, such as heart rate, blood pressure, blood oxygen, blood sugar and other indicators to a smart Healthcare platform. The platform stores this information on the blockchain, and then recommends suitable doctors to patients through a doctor recommendation system [14], which is granted access to patient data only with the patient's consent. To ensure privacy, each **DO** encrypts his/her own health data and stores the encrypted ciphertext to IPFS, which will send the storage address back to the **DO**. Then, the appropriate **DU** will be recommended using data mining [34]. If the **DO** decides to authorize the **DU**, then the access control policy Ψ is set and recorded on the blockchain. Once being authorized, the **DU** will be granted the permission. Meanwhile, the ciphertext storage address will be sent to the **DU**, using which the corresponding ciphertext is downloaded and then decrypted. Thus, the **DU** can make timely diagnosis. It is worth to mention that before making the request, the **DU**'s identity should be checked to ensure that he/she is a legitimate user.

The symbols and their descriptions used throughout this paper are listed in Table I.

TABLE I
SYMBOL DESCRIPTION.

Symbols	Descriptions
e_p	Finite field
g	The base point on the elliptic curve
h	Hash function
u_{id}	User's Identity
m_u	User's information
ν_u	User's signature
pk_e	User's Ethereum public key
sk_e	User's Ethereum private key
sk_u	User's private key
pk_u	User's public key
m_{hd}	Health data
$c_.$	Ciphertext
δ	Download address

V. THE IMPLEMENTATION DETAILS OF THE PROPOSED SCHEME

The proposed scheme is composed of the following modules, namely the information registration, identity authentication, health data storage, doctor recommendation, health data access request and authorization, and decrypt and obtain data.

A. Information Registration

User **u** must first register with the **TA**. To be specific, the **TA** obtains the user's private key and calculates the user's public key. Then, the private key, the public key and a unique identity u_{id} are generated for the user. Finally, the **TA** saves the encrypted private key and u_{id} on the blockchain and sends the u_{id} to the user **u**, who obtains his/her private key from the blockchain. The details of the above process is specified as follows:

First, the personal information m_u is signed by the user **u** with Ethereum private key sk_e, the signature of which is denoted by ν_u. Meanwhile, the user sends Ethereum public key pk_e, m_u and ν_u to the **TA** as the registration request information, i.e.,

$$\begin{aligned} req &= (m_u, pk_e, \nu_u), \\ \nu_u &= sign(m_u, sk_e). \end{aligned} \tag{2}$$

After receiving req, the **TA** first verifies the signature information ν_u with pk_e. If the verification is successful, then the Ethereum account address $addr_e$ is obtained from the pk_e; otherwise, an error message is returned to the user **u**.

Then, the **TA** checks whether the Ethereum address has been occupied while interacting with the smart contract. If it is not, the **TA** calculates the user's public key $pk_u = sk_u \cdot g$, by randomly selecting $sk_u \in e_p$ as the user's private key, and generates a unique identifier for the user by

$$u_{id} = h\big((sk_u, pk_u), h(m_u)\big). \tag{3}$$

Meanwhile, it encrypts sk_u with pk_e to obtain ciphertext c_{sk_u}, calls the smart contract to store $addr_e$, c_{sk_u} and u_{id} on blockchain, and sends the u_{id} back to the user $\mathbf{u}$.

Finally, the user call the smart contract to find the corresponding identity u_{id} according to his/her Ethernet address $addr_e$, after receiving the information. If $u_{id}^{'} = u_{id}$, then the smart contract sends c_{sk_u} to the user $\mathbf{u}$, who will decrypt the private key sk_u with the Ethereum account private key sk_e, which provides data support for subsequent identity authentication. The information registration is summarized in Algorithm 1.

Algorithm 1 User Registration

Input: the user information m_u; User signature ν_u; User Ethereum public key pk_e
Output: allow or deny

calculate the signature $\nu_u^{'} = sign\big(h(m_u), pk_e\big)$
if $\nu_u^{'} = \nu_u$ **then**
  $addr_e = GetEthAddress(pk_e)$
  if IsExist($addr_e$) = false **then**
    select $sk_u \in e_p$
    calculate $pk_u = sk_u \cdot g$
    calculate $u_{id} = h\big((sk_u, pk_u), h(m_u)\big)$
    calculate $c_{sk_u} = enc(sk_u, pk_e)$
    storage $\{addr_e, c_{sk_u}, u_{id}\}$ to blockchain
    return u_{id}
  end if
else
  return exist
else
  return error
end if

B. Identity Authentication

During user authentication, the user needs to send the request information with the digital signature to the server. If it is invalid, then the identity authentication is interrupted; otherwise, the zero-knowledge proof is used for identity authentication.

To be specific, user $\mathbf{u}$ first sends the digital signature to the server. Then, the server verifies if the digital signature is correct. If it is, then the zero-knowledge identity authentication is performed as follows. User $\mathbf{u}$ randomly selects $k \in e_p$, calculates $r = k \cdot g$, and sends it to the server. Once the server receives r, randomly selects $q \in e_p$, converts it into hexadecimal r_h, and sends it back to user $\mathbf{u}$. Next, user $\mathbf{u}$ calculates $v = k + r_h \cdot sk_u$ after receiving the random number r_h, and returns it to the server. Then, the server verifies the correctness of the $vg = r + r_h \cdot pk_u$ for identity authentication. Naturally, If the authentication is valid and the user is correctly identified, then the request is approved; otherwise, the request is denied.

C. Health Data Storage

In our case, the wearable devices collect the user's health data. To encrypt the health data m_{hd}, we choose AES as the symmetric encryption algorithm, i.e.,

$$c_{m_{hd}} = enc(m_{hd}, k_{AES}). \tag{4}$$

After the data owner $\mathbf{DO}$ encrypts the data, the AES key k_{AES} is stored locally. To verify the integrity of the encrypted data block, the hash value of the encrypted data is calculated. Meanwhile, the $\mathbf{DO}$ signs the encrypted data with his/her private key to provide data authentication. Then, the $\mathbf{DO}$ stores the signature, denoted by $\sigma = sign(c_{m_{hd}})$, and the encrypted data $c_{m_{hd}}$ in IPFS. Then, IPFS returns the download address δ of the data to the $\mathbf{DO}$. Finally, the $\mathbf{DO}$ store data $\{u_{id}, \delta, h, \sigma\}$ on the blockchain. The process of health data storage is summarized in Algorithm 2.

Algorithm 2 Health Data Storage

Input: the user health data m_{hd}
Output: success or failure

calculate the ciphertext $c_{m_{hd}} = enc(m_{hd}, k_{AES})$
store AES key k_{AES}
calculate the hash value $h = h(c_{m_{hd}})$
calculate the signature $\sigma = sign(c_{m_{hd}})$
δ =IPFS($c_{m_{hd}}, \sigma$)
store data $\{u_{id}, \delta, h, \sigma\}$ on the blockchain
return success or failure

D. Doctor Recommendation

The design of the medical recommendation system [35], [36] can make a preliminary diagnosis of the patient's condition by recommending a suitable doctor for the patient. For example, PPMR [37] takes the reputation score of doctors, the similarity between user needs and doctor information as the basis for medical service recommendation, and the reputation score of doctors is measured through user feedback. MDCM [38] is a multi-modal deep computation model designed for syndrome recognition that is a crucial part of syndrome differentiation. DRMP [39] introduces gating mechanisms based on the knowledge of drug-drug interaction and Bayesian neural networks, which enable it to make multiple recommendations for patients and provide confidence in each recommendation result. However, all these algorithms focus on optimizing the single doctor-patient pairing. To solve this problem, the deep reinforcement learning [40] algorithm DQN is employed for doctor recommendation with the consideration of maximizing patient-doctor matching degree on average.

In the DQN based doctor recommendation, we let the selection of doctors consist of the state s. That is, $s = (c_1, c_2, \ldots, c_n)$, where $c_i \in (0, 1)$ represents whether the ith doctor is chosen or not. We consider that every doctor has his own field of expertise d_i, i.e., $d_i = \{e_1, e_2, \ldots, e_n\}$, where e_j represents the jth disease. If the ith doctor's expertise set can intersect with the jth patient's syndrome set p_j to a certain extent, then the doctor may be recommended to this patient. According to the above analysis, we give the definition of matching degree $m_{i,j}$ about the ith doctor and the jth patient as follows:

$$m^{i,j} = \frac{\big|F(d_i) \cap p_j\big|}{\big|p_j\big|}, \tag{5}$$

where $F(.)$ is the function that maps diseases to their syndromes. According to this definition, we only need to find a reasonable threshold value, and when the doctor-patient matching degree is higher than the threshold value, we recommend this doctor to the patient. Therefore, we use the threshold θ as the action a, i.e., $a = \theta$. Since the platform needs to recommend doctors to multiple patients, we use the average matching degree as the reward γ to measure the quality of the recommendation algorithm for M doctors and N patients, i.e.,

$$\gamma = \frac{1}{N} \sum_{i=1}^{M} \sum_{j=1}^{N} m^{\mathbf{1}_{i,j}}, \tag{6}$$

where $m^{\mathbf{1}_{i,j}}$ denotes the matching degree (5) under the recommendation condition given by

$$\mathbf{1}_{i,j} = \begin{cases} 1 & if\ doctor\ i\ is\ recommendated\ for\ patient\ j \\ 0 & otherwise. \end{cases} \tag{7}$$

To get the optimal doctor recommendation policy π, the Q-network is trained using supervised learning with the loss function given by

$$L(\omega) = \left[\gamma_t + \beta max_{a_{t+1}} \hat{Q}(s_{t+1}, a_{t+1}; \omega^-) - Q(s_t, a_t; \omega)\right]^2, \tag{8}$$

where s_t, a_t and γ_t denote the state, action and reward at the time step t during the recommendation threshold decision process, respectively; β is the learning rate; ω and ω^- are the parameters of the Q-network and target Q-network, and the Q value of which are denoted by Q and $\hat{Q}$, respectively. The proposed DQN based doctor recommendation procedure is summarized in Algorithm 3.

Algorithm 3 DQN based Doctor Recommendation

Input: initialize replay memory D, action-value Q and $\hat{Q}$ with random weights ω and ω^-
Output: doctor recommendation policy π

Initialize
for $episode = 1, M$ **do**
  Initialize state s_1
  for $t = 1, T$ **do**
    Select a random action a_t with probability ϵ , otherwise $a_t = max_a Q^*(s_t, a; \omega)$
    Get reward γ_t and next state s_{t+1} after executing a_t
    The transition $(s_t, a_t, \gamma_t, s_{t+1})$ is stored in D
    Sample random minibatch of transitions $(s_t, a_t, \gamma_t, s_{t+1})$ from D
    Set $y_t = \begin{cases} \gamma_t\ (6) & if\ episode\ ends\ at\ step\ t+1 \\ \gamma_t + \beta max_{a_{t+1}} \hat{Q}(s_{t+1}, a_{t+1}; \omega^-) & otherwise \end{cases}$
    Update $\left(y_t - Q(s_t, a_t; \omega)\right)^2$ using gradient descent method for ω
    Update the target Q-network every $\mathcal{T}$ steps, $\omega^- = \omega$
  end for
end for

E. Health Data Access Request and Authorization

The $\mathbf{DU}$ first pass the authentication of the edge server. When the $\mathbf{DU}$ requests access to health data, the whole access control process is divided into two stages, namely permission judgment and access authorization. To be specific, the permission judgment stage is used to query roles and access control policies, while the access authorization stage is used to grant the data owner $\mathbf{DO}$ access rights. We summarize both stages as follows:

First, we verify whether the $\mathbf{DU}$ has the right to access the data. The authority determination contract queries its own authority according to the u_{id} of the $\mathbf{DU}$. If there is an access policy Ψ set by the $\mathbf{DO}$, it is determined as passed. After the permission is verified, the $\mathbf{DU}$ can obtain $data = \{u_{id}, \delta, h, \sigma\}$ stored in the blockchain and send an access request to the $\mathbf{DO}$, which is summarized in Algorithm 4.

Algorithm 4 Access Rights Check

Input: the user identity of data owner u_{id}; User role set $user\_role$; Role permission set $role\_permission$
Output: allow or deny

set $roles$=[], $permissions$=[]
for $i = 1, user\_role.length$ **do**
  if $user\_role[i].uid = u_{id}$ **then**
    $roles.push(user\_role[i])$
  end if
end for
for $m = 1, roles.length$ **do**
  for $j = 1, role\_permission.length$ **do**
    if $role\_permission[j].role = roles[m]$ **then**
      $permissions.push\big(role\_permission[j]\big)$
    end if
  end for
end for
if $permissions$ is null **then**
  return deny
else
  return allow
end if

After the $\mathbf{DO}$ receives the access request, if he/she agrees, then the following process will be performed. Specifically, $\mathbf{DO}$ randomly selects $r \in e_p$, and calculates

$$\begin{aligned} c_1 &= rg, \\ c_2 &= k_{AES} + r \cdot pk_u. \end{aligned} \tag{9}$$

Then, $\mathbf{DO}$ sends $c = \{c_1, c_2\}$ to the $\mathbf{DU}$ via the edge server.

F. Decrypt and Obtain Data

Once obtaining the $\mathbf{DO}$'s authorization, the $\mathbf{DU}$ can use his/her private key sk_u to decrypt the symmetric key k_{AES}, and obtain the ciphertext $c_{m_{hd}}$ from IPFS according to the download address δ.

$$\begin{aligned} c_2 - sk_u \cdot c_1 &= k_{AES} + r \cdot pk_u - sk_u \cdot rg \\ &= k_{AES}. \end{aligned} \tag{10}$$

After obtaining the ciphertext $c_{m_{hd}}$ and the symmetric key k_{AES}, the $\mathbf{DU}$ calculates the hash value $h^{'}$ by

$$h^{'} = h(c_{m_{hd}}). \tag{11}$$

If $h^{'} = h$, then the $c_{m_{hd}}$ is proved that it has not been tampered with. Then, the $\mathbf{DU}$ decrypts the ciphertext $c_{m_{hd}}$ with k_{AES} to obtain the $\mathbf{DO}$'s health data by

$$m_{hd} = dec(C_{m_{hd}}, k_{AES}). \tag{12}$$

VI. Theoretical Analysis on Security and Performance

In this section, we give the theoretical analysis to prove the security of the proposed scheme in terms of introducing the attacks prevented. We also analyze the cost of the proposed scheme in both computation and communication.

A. Security Analysis

The identity authentication is to make the verifier believe the identity of the certifier without disclosing personal information, and the security of which depends on that of elliptic curve discrete logarithm and zero knowledge proof. By introducing the following attacks, namely single point of failure attack, tamper attack, replay attack, impersonation attack, and collusion attack, and conducting theoretical analysis, we prove that the proposed scheme can resist these attacks.

- Single Point of Failure Prevention [19]: Because the blockchain is a distributed ledger, each full node will store all the information in the chain, which can prevent the failure of centralized applications. A few node failures will not affect the operation of the entire system.
- Tamper Resistance [41]: Because the scheme exists in the blockchain network, and the blockchain system is decentralized, the transactions in the blockchain are transparent and cannot be tampered with, which can ensure that the user's identity credentials and related transactions will not be maliciously tampered with, thus ensuring the integrity of the user's information.
- Replay Attack [42]: This attack randomly selects different random numbers during each authentication process. So attacker $\mathbf{A}$ tries to listen to all the information exchanged during an authentication process, and he/she cannot fool authenticator $\mathbf{V}$ by resending outdated messages. Thereby, it is effectively against any replay attack.
- Impersonation Attack [43]: In such attack, attacker $\mathbf{A}$ pretends to be prover $\mathbf{P}$ to make an interactive request to verifier $\mathbf{V}$, but attacker $\mathbf{A}$ does not have the private key of prover $\mathbf{P}$. If $\mathbf{A}$ forges the signature, the attacker cannot pass the signature verification; if $\mathbf{A}$ intercepts the signature, the attacker cannot pass the zero-knowledge authentication process. In this scheme, if the attacker $\mathbf{A}$ intercepts r and g, the difficulty of deriving k from $r = kg$ is equivalent to the difficulty of solving the elliptic curve discrete logarithm problem ECDLP. If v is intercepted, deriving sk_u from $v = k + r_h \cdot sk_u$ also belongs to solving ECDLP, which is also very difficult. Because k and r_h are randomly generated during the authentication process, and each authentication process will produce different values.
- Collusion Attack [44]: Malicious verifier $\mathbf{V}$ colluded with attacker $\mathbf{A}$, and the malicious verifier $\mathbf{V}$ told attacker $\mathbf{A}$ all the obtained information of prover $\mathbf{P}$ in the authentication. However, in the zero-knowledge authentication, the malicious verifier can only get r and v, but cannot get the private key information of prover $\mathbf{P}$. If the attacker $\mathbf{A}$ wants to obtain the private key of prover $\mathbf{P}$ from v, its difficulty is equivalent to the difficulty of obtaining elliptic curve. Therefore, attacker $\mathbf{A}$ can hardly crack in the limited time.

According to the above analysis, we claim that the proposed scheme can resist malicious forgery, impersonation and disclosure, thus it has considerably high security.

B. Performance Analysis

Both of the computation overhead and communication overhead of the proposed scheme are analyzed as follows:

- Computation Overhead: Let $\mathcal{T}_m$, $\mathcal{T}_h$, and $\mathcal{T}_{code}$ represent the cost of the last point multiplication operation of group g on the elliptic curve, a hash function operation, and running an encryption or decryption operation, respectively. Thus, the calculation overhead of registration phase and authentication phase equals to $\mathcal{T}_m + 2\mathcal{T}_h + \mathcal{T}_{code}$ and $3\mathcal{T}_m$, respectively. And, recommending the appropriate doctors through DQN is equivalent to solving the set coverage problem with the same scale in terms of computation overhead. Among them, the number of doctors is M, and the number of patients is N. If the greedy algorithm is adopted, then the computation overhead of finding an approximate solution for a set coverage problem is the order of M^2, denoted by $\mathcal{T}_{dqn}$, which bounds that of the DQN-based doctor recommendation algorithm.
- Communication Overhead: Let $\mathcal{L}_{id}$, $\mathcal{L}_{sign}$, and $\mathcal{L}_p$ represent the length of identity information, user signature, and element in e_p, respectively. In the registration stage, the length of the registration information $req = (m_u, pk_e, \nu_u)$ sent by the user is $\mathcal{L}_{id} + \mathcal{L}_{sign} + \mathcal{C}$, where $\mathcal{C}$ represent a constant, while the length of the response information u_{id} returned by the authentication server is $\mathcal{L}_{id}$. Thus, to complete the user registration, the total communication cost equals to $2\mathcal{L}_{id} + \mathcal{L}_{sign} + \mathcal{C}$. In the authentication phase, the user sends the signature information to the user with a length of $\mathcal{L}_{sign}$. After the signature verification is passed, the authentication server returns a message agreeing to zero knowledge authentication with a length of $\mathcal{C}$. The user sends login authentication request information $r = kg$ with a length of $\mathcal{L}_p$, while the length of the response information r returned by the authentication server is $\mathcal{L}_p$. In addition, the length of the information v sent by the user to the authentication server is also $\mathcal{L}_p$. When the authentication is passed, the authentication server sends the authentication information to the user with a length of $\mathcal{C}$. Thus, the communication overhead required to complete an identity authentication equals to $3\mathcal{L}_p + 2\mathcal{C} + \mathcal{L}_{sign}$.

Since the DQN-based doctor recommendation algorithm needs to collect patient disease and doctor expertise data for training, the communication overhead equals to $\sum_{i=1}^{M} \mathcal{L}_{d_i} + \sum_{j=1}^{N} \mathcal{L}_{p_j}$, where $\mathcal{L}_{d_i}$ and $\mathcal{L}_{p_j}$ represent the length of the ith doctor's expertise and the length of the jth patient's syndrome, respectively.

VII. Performance Evaluation

A. Experiment Setup

In this section, we conduct the experiment on a computer with Intel Core i5 processor, 8G memory, 3.2GHz CPU frequency and Ubuntu system. We use the Solidity language to compile smart contracts, then compile smart contracts in the online compilation environment Remix, and finally build a private chain to deploy smart contracts through Ganache. In addition, we use JPBC2.0.0 library and Java development language to implement zero-knowledge authentication scheme based on elliptic curve. The DQN network used in the experiment consists of an input layer, three hidden layers, and an output layer. The activation function is relu with a learning rate of 1e-3.

Performance evaluation adopts the following performance indicators, namely throughput, delay, data encryption and decryption time consumption, and upload and download time consumption. We also evaluate the performance of the proposed doctor recommendation algorithm in terms of average matching degree. The dataset used in the experiment contains the information data of 151,989 doctors in 5,024 hospitals in China, which is available at "http://n3.datasn.io/data/api/v1/n3a2/hospital_clinic_doctor_in_china/main/list/?app=html-bunker", including doctor's title, expertise, peer evaluation, patient evaluation, etc. We grade the doctor's ability according to the doctor's expertise. That is, each doctor's ability is scored according to his/her expertise, with a score range of 0 to 100. In addition, we use the Ethereum private chain as the experimental environment, the configuration of which is shown in Table II.

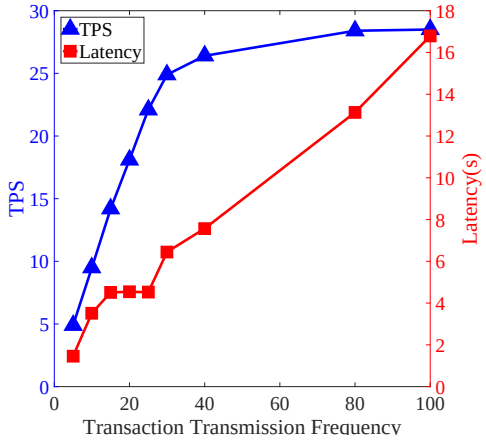
TABLE II
Test Environment.

Parameter	*Version*
Geth	1.10.12-stable
The operation system	Ubuntu20.04
IPFS	0.12.0
Solidity	0.5.0
Node.js	V14.18.1

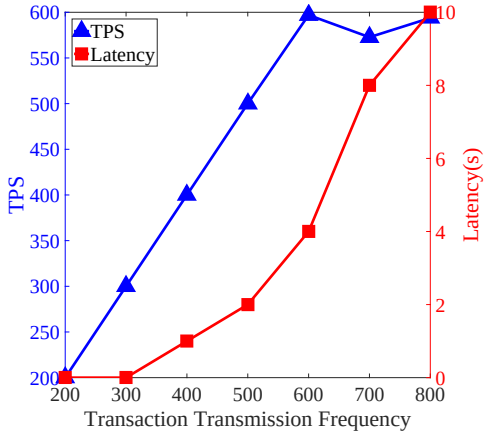
B. Experiment Results

The performance of the proposed scheme is evaluated in terms of Ethereum network performance, user identity authentication and access control efficiency, data processing efficiency, and smart contract deployment cost.

1) Ethereum Network Performance: The Ethereum private chain runs on a single host. The test method is to send 1000 transactions to Ethereum, set the transaction type to write and query, and then observe the change results of the average system delay and throughput under different transaction transmission frequencies. The results are shown in Figure 2 (a) and Figure 2 (b). As shown in these figures, when the transaction type is write, there is no significant change in latency when the transaction transmission frequency falls within the range of 0∼30. However, with the increase of transaction transmission frequency, the average delay increases gradually. When the transaction transmission frequency reaches 80, the throughput tends to be stable. When the transaction type is query, the change of average delay is not obvious and can be ignored. The throughput is maximized at 600 transaction transmission frequencies. This is because when the transaction type is write, Ethereum needs nodes to consume gas synchronously, and the increased transaction volume needs to be queued for verification.



(a)



(b)

Fig. 2. Effect of transaction transmission frequency on (a) write and (b) query performance.

2) User Identity Authentication and Access Control Efficiency: Both ECC and RSA encryption algorithm are considered in the experiment, wherein ECC uses 256 bits of

This article has been accepted for publication in IEEE/ACM Transactions on Computational Biology and Bioinformatics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCBB.2023.3281819

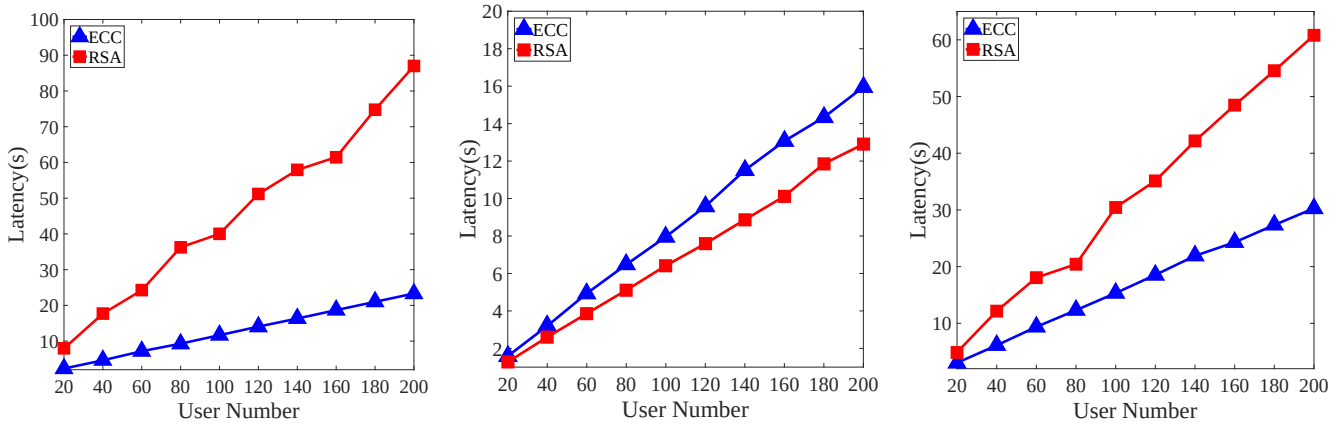


Fig. 3. Latency comparison between ECC and RSA with user number varies from 20 to 200 in (a) user identity registration, (b) user signature verification, and (c) user identity authentication.

encryption length and RSA uses 2048 bits of encryption length. And the transaction efficiency of user registration and authentication stage is analyzed.

In the user identity registration stage, the trusted authorization center performs experimental verification of user public and private keys and signature generation based on ECC and RSA encryption algorithms respectively according to the registration information submitted by users. The verification latency is shown in Figure 3 (a). Observed from this Figure, as the number of users increases, the latency of the registration phase of user identity information is also increasing. The time consumed for user identity registration based on RSA increases rapidly with the number of users, and the processing efficiency is relatively low. The time consumed by ECC user identity information registration grows slowly. Both of user signature verification and user identity authentication are performed based on ECC and RSA and the experimental results are shown in Figure 3 (b) and Figure 3 (c), respectively. It is clear that RSA spent more time in the signature verification phase than ECC. Note that in user authentication, both checks and verifications are performed. Therefore, in the whole authentication process, the processing efficiency of ECC is higher than that of RSA. In addition, as the number of users increases, the latency of user identity registration and authentication increases linearly, because users need to queue for processing.

The average matching degree comparison between the proposed scheme and the baselines PPMR [37] and MDCM [38] are shown in Figure 4 (a) and 4 (b). Note that the PPMR algorithm is to recommend the doctor with the highest credit rating after the doctor's ability reaches a certain threshold, while MDCM maps the multimodal symptoms of a patient to the most appropriate doctor which is somehow similar to our approach. Since the doctor credit is not considered in this paper, the PPMR will select doctors whose ability exceeds the threshold to adapt to the current test environment. As can be seen from Figure 4 (a), the higher the ability of doctors, the higher the average matching degree when the number of pa-

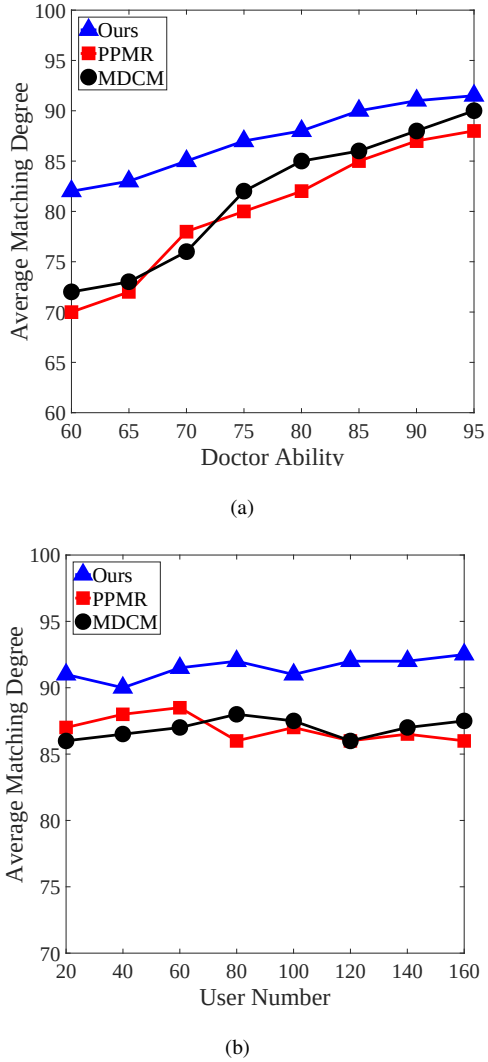


Fig. 4. Average matching degree comparison with the variation of (a) doctor ability and (b) user number.

tients is set to 160. The average matching degree of our scheme is significantly higher than that of both PPMR and MDCM as we expected. This is because our scheme optimizes the doctor recommendation by maximizing the average matching degree, while both baseline algorithms focus on optimizing the single doctor-patient pairing. As can be seen from Figure 4 (b), the average matching degree of either approach experiences a little fluctuation as the number of patients increases with the ability of each doctor reaches 95. Although both PPMR and MDCM have successfully reached their highest average matching degrees, 88% and 87%, respectively, due to almost all doctors have the ability to cure every disease, our scheme is still about 5% higher than PPMR and about 6% higher than MDCM. The results shown in Figure 4 suggest that the proposed scheme can provide better doctor recommendation services for patients.

3) Data Processing Efficiency: As can be seen from Figure 5, because of the symmetric encryption algorithm AES, the encrypted file size is about twice the size of the raw file for all 6 files. As a result, the time required to decrypt the file is higher than the encryption time as shown in Figure 6.

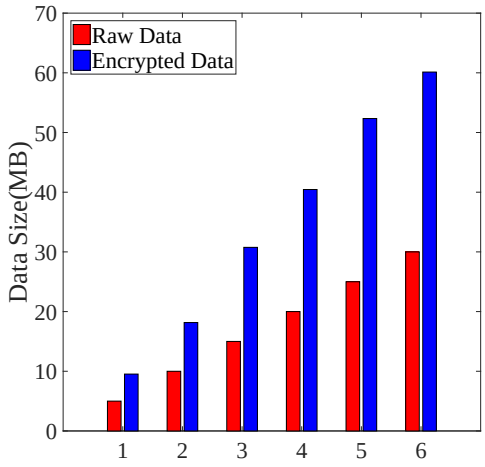


Fig. 5. Data size comparison between raw data and encrypted data.

This experiment calculates the time of data encryption and decryption by changing the size of health data block, and evaluates the computational overhead in the data management system. As shown in Figure 6, the computation cost of encryption and decryption algorithm has no great impact on the calculation cost of encryption and decryption algorithm. In addition, as the size of the health data block increases, the running time increases slowly, which shows that the computation overhead of this scheme is controllable. It can also be observed from this figure that the size of the health data block should not exceed 15MB, so as to reduce the computation overhead of the system.

Observed from Figure 7, we find that as the data size increases, it will take more time to upload or download data from the IPFS system, but the time consumed is still within the acceptable range. Even if the size of the ciphertext data is 60MB, it only takes 0.778 seconds to complete the upload and 0.355 seconds to download. In particular, we find that it only

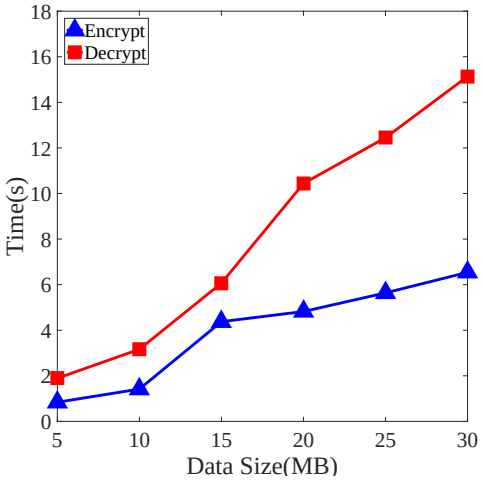


Fig. 6. Time consumption comparison between encryption and decryption of files with different data sizes.

takes 18.534 seconds to upload 1G data to the IPFS system and 10.436 seconds to download.

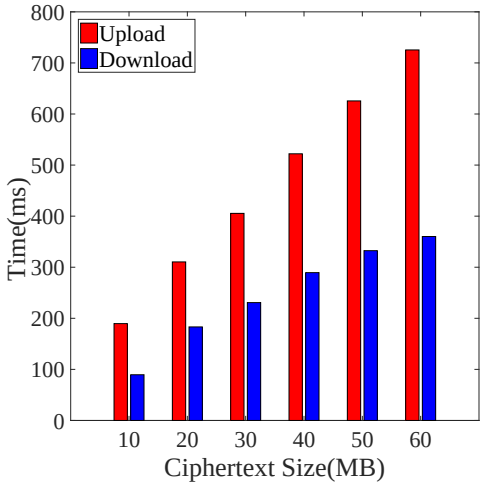


Fig. 7. Time consumption comparison between upload and download of ciphertexts with different data sizes.

4) Smart Contract Deployment Cost: We use solidity to store patient health data information and control user permissions. The contract is deployed on the private chain network of Ethereum and tested with MetaMask wallet. We also test the gas consumption of the main functions on the smart contract and the system response time when calling the smart contract functions. The test results are shown in Table III, which indicate that the response time of each system is about 2 seconds.

VIII. Conclusion

Under the influence of the COVID-19, more and more medical care professionals and patients use medical wearable devices for diagnosis and treatment, which simplifies and improves the diagnosis and treatment process. However, the

TABLE III
SMART CONTRACT DEPLOYMENT.

Smart Contract Function	Gas Cost	Response Time (ms)
registerPatient	43828	1826.45
registerDoctor	48095	2120.24
uploadData	245054	2736.38
sendRequestToPatient	53408	2687.68
agreeAccess	50146	1887.49
revokeAccess	35278	2942.67
getData	0	27.63

patients' private information may be leaked due to improper use of medical data. In this paper, a new blockchain-based data access security scheme is designed to solve this problem. The scheme combines blockchain, elliptic curve encryption and zero-knowledge proof to protect patients' medical data privacy. To provide better treatment, the DQN algorithm is employed to recommend appropriate doctors for patients. Thus, only authenticated patients can access the blockchain network and store their medical data, while authenticated doctors can access patients' health data after obtaining their authorizations. The experimental results along with security analysis demonstrate that our scheme can effectively protect patients' data privacy during treatment through secure authentication and data access for medical wearables.

Our future works focus on the management of visitors' rights, and the access rights management scheme will be improved to strengthen privacy protection and security.

ACKNOWLEDGMENT

This work is supported by National Natural Science Foundation of China under Grant No. 61702103 and U1905211, and Natural Science Foundation of Fujian Province under Grant No. 2020J01167 and 2020J01169.

REFERENCES

[1] E. Hosseini, K. Z. Ghafoor, A. S. Sadiq, M. Guizani and A. Emrouznejad, "Covid-19 optimizer algorithm, modeling and controlling of coronavirus distribution process," *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 10, pp. 2765-2775, 2020.

[2] S. Liu, X. Wang, L. Zhao, J. Zhao, Q. Xin and S. -H. Wang, "Subject-independent emotion recognition of EEG signals based on dynamic empirical convolutional neural network," *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, vol. 18, no. 5, pp. 1710-1721, 2021.

[3] A. Talitckii et al., "Avoiding misdiagnosis of Parkinson's disease with the use of wearable sensors and artificial intelligence," *IEEE Sensors Journal*, vol. 21, no. 3, pp. 3738-3747, 2021.

[4] S. I. Lee et al., "Predicting and monitoring upper-limb rehabilitation outcomes using clinical and wearable sensor data in brain injury survivors," *IEEE Transactions on Biomedical Engineering*, vol. 68, no. 6, pp. 1871-1881, 2021.

[5] A. Krall, D. Finke and H. Yang, "Mosaic privacy-preserving mechanisms for healthcare analytics," *IEEE Journal of Biomedical and Health Informatics*, vol. 25, no. 6, pp. 2184-2192, 2021.

[6] R. Sánchez-Guerrero, F. A. Mendoza, D. Díaz-Sánchez, P. A. Cabarcos and A. M. López, "Collaborative ehealth meets security: Privacy-enhancing patient profile management," *IEEE Journal of Biomedical and Health Informatics*, vol. 21, no. 6, pp. 1741-1749, 2017.

[7] Jin H, Luo Y, Li P, et al., "A review of secure and privacy-preserving medical data sharing," *IEEE Access*, vol. 7, pp. 61656-61669, 2019.

[8] R. S. Sandhu, E. J. Coyne, H. L. Feinstein and C. E. Youman, "Role-based access control models," *Computer*, vol. 29, no. 2, pp. 38-47, 1996.

[9] E. Yuan and J. Tong,"Attributed based access control (ABAC) for Web services," *IEEE International Conference on Web Services (ICWS'05)*, 2005, pp. 569.

[10] R. K. Thomas, R. S. Sandhu, "Task-based authorization controls (TBAC): A family of models for active and enterprise-oriented authorization management," *DBSec*, vol. 113, pp. 166-181, 1997.

[11] K. Edemacu, B. Jang and J. W. Kim, "Collaborative ehealth privacy and security: An access control with attribute revocation based on OBDD access structure," *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 10, pp. 2960-2972, 2020.

[12] X. Wang, S. Garg, H. Lin, G. Kaddoum, J. Hu and M. S. Hossain, "A secure data aggregation strategy in edge computing and blockchain-empowered internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14237-14246, 2022.

[13] B. S. Egala, A. K. Pradhan, V. Badarla and S. P. Mohanty, "Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control," *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11717-11731, 2021.

[14] X. Zhou, W. Liang, K. Wang and S. Shimizu, "Multi-modality behavioral influence analysis for personalized recommendations in health social media environment," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 5, pp. 888-897, 2019.

[15] L. Axon, "Privacy-awareness in blockchain-based PKI," *CDT Technical Paper Series* 21/15, 2015.

[16] L. Axon and M. Goldsmith, "PB-PKI: A privacy-aware blockchain-based PKI," *SCITEPRESS*, vol. 6, 2016.

[17] M. Ali, J. Nelson, R. Shea and M. J. Freedman, "Blockstack: A global naming and storage system secured by blockchains," *In Proceedings of the 2016 USENIX Annual Technical Conference, USENIX ATC 2016*, 2016, pp. 181-194.

[18] T. Bui and T. Aura, "Application of public ledgers to revocation in distributed access control," *In International Conference on Information and Communications Security*, Springer, Cham, 2018, pp. 781-792, doi: 10.1007/978-3-030-01950-1_48.

[19] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," *2016 2nd International Conference on Open and Big Data (OBD)*, 2016, pp. 25-30, doi: 10.1109/OBD.2016.11.

[20] A. Ekblaw, A. Azaria, J. D. Halamka and A. Lippman, "A case study for blockchain in healthcare:"MedRec" prototype for electronic health

records and medical research data," *In Proceedings of IEEE open & big data conference*, 2016, vol. 13, pp. 13.

[21] H. Guo, W. Li, M. Nejad and C. Shen, "Access control for electronic health records with hybrid blockchain-edge architecture", *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019, doi: 10.1109/blockchain.2019.00015.

[22] L. Song, M. Li, Z. Zhu, P. Yuan and Y. He, "Attribute-based access control using smart contracts for the internet of things", *Procedia Computer Science*, vol. 174, pp. 231-242, 2020.

[23] T. Sultana, A. Ghaffar, M. Azeem, Z. Abubaker, M. Gurmani and N. Javaid, "Data sharing system integrating access control based on smart contracts for IoT", *Advances on P2P, Parallel, Grid, Cloud and Internet Computing*, pp. 863-874, 2019.

[24] A. Liu, X. Du and N. Wang, "Efficient access control permission decision engine based on machine learning", *Security and Communication Networks*, vol. 2021, pp. 1-11, 2021.

[25] B. Tay and A. Mourad, "Intelligent performance-aware adaptation of control policies for optimizing banking teller process using machine learning", *IEEE Access*, vol. 8, pp. 153403-153412, 2020.

[26] C. Esposito, M. Ficco and B. Gupta, "Blockchain-based authentication and authorization for smart city applications", *Information Processing & Management*, vol. 58, no. 2, p. 102468, 2021.

[27] G. Fragkos, J. Johnson and E. E. Tsiropoulou, "Dynamic Role-Based Access Control Policy for Smart Grid Applications: An Offline Deep Reinforcement Learning Approach," *IEEE Transactions on Human-Machine Systems*, vol. 52, no. 4, pp. 761-773, 2022.

[28] X. Liu, H. Zhang, K. Long, A. Nallanathan and V. C. M. Leung, "Deep Dyna-Reinforcement Learning Based on Random Access Control in LEO Satellite IoT Networks," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14818-14828, 2022.

[29] H. Lin, K. Kaur, X. Wang, G. Kaddoum, J. Hu and M. M. Hassan, "Privacy-Aware Access Control in IoT-Enabled Healthcare: A Federated Deep Learning Approach," *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 2893-2902, 2023.

[30] T. Meng, Y. Zhao, K. Wolter and C. -Z. Xu, "On consortium blockchain consistency: A queueing network model approach," IEEE Transactions on Parallel and Distributed Systems, vol. 32, no. 6, pp. 1369-1382, 2021.

[31] R. Amiri and O. Elkeelany, "FPGA design of elliptic curve cryptosystem (ECC) for isomorphic transformation and EC ElGamal encryption," *IEEE Embedded Systems Letters*, vol. 13, no. 2, pp. 65-68, 2021.

[32] D. Mouris and N. G. Tsoutsos, "Zilch: A framework for deploying transparent zero-knowledge proofs," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3269-3284, 2021.

[33] X. Zhou, X. Xu, W. Liang, Z. Zeng, and Z. Yan, "Deep-learning-enhanced multitarget detection for end-edge-cloud surveillance in smart IoT," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12588-12596, 2021.

[34] X. Zhou, W. Liang, K. Wang, and L. T. Yang, "Deep correlation mining based on hierarchical hybrid networks for heterogeneous big data recommendations," *IEEE Transactions on Computational Social Systems*, vol. 8, no. 1, pp. 171-178, 2021.

[35] Y. Jin, W. Ji, W. Zhang, X. He, X. Wang and X. Wang, "A kg-enhanced multi-graph neural network for attentive herb recommendation," *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, doi: 10.1109/TCBB.2021.3115489.

[36] X. Zhou, Y. Li and W. Liang, "CNN-RNN based intelligent recommendation for online medical pre-diagnosis support," *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, vol. 18, no. 3, pp. 912-921, 2021.

[37] C. Xu, J. Wang, L. Zhu, C. Zhang and K. Sharif, "PPMR: a privacy-preserving online medical service recommendation scheme in eHealthcare system," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5665-5673, 2019.

[38] Q. Zhang, C. Bai, L. T. Yang, Z. Chen, P. Li and H. Yu, "A Unified Smart Chinese Medicine Framework for Healthcare and Medical Services," *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, vol. 18, no. 3, pp. 882-890, 2021.

[39] Y. Ren, Y. Shi, K. Zhang, X. Wang, Z. Chen and H. Li, "A Drug Recommendation Model Based on Message Propagation and DDI Gating Mechanism," *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 7, pp. 3478-3485, 2022.

[40] X. Zhou, W. Liang, K. Yan, W. Li, K. Wang, J. Ma, and Q. Jin, "Edge enabled two-stage scheduling based on deep reinforcement learning for internet of everything," *IEEE Internet of Things Journal*, 2022, doi: 10.1109/JIOT.2022.3179231.

[41] Chen Y, Ding S, Xu Z, et al., "Blockchain-based medical records secure storage and medical service framework," *Journal of medical systems*, vol. 43, no. 1, pp. 1-9, 2019.

[42] I. Fernández-Hernández and G. Seco-Granados, "Galileo NMA signal unpredictability and anti-replay protection," *2016 International Conference on Localization and GNSS (ICL-GNSS)*, 2016, pp. 1-5, doi: 10.1109/ICL-GNSS.2016.7533686.

[43] S. Tu et al., "Reinforcement learning assisted impersonation attack detection in device-to-device communications," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1474-1479, 2021.

[44] S. Cui, S. Belguith, P. De Alwis, M. R. Asghar and G. Russello, "Collusion defender: preserving subscribers' privacy in publish and subscribe systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 3, pp. 1051-1064, 2021.

Hui Lin is a professor in the College of Computer and Cyber Security at the Fujian Normal University, Fuzhou, China. He received his Ph.D. degree in Computing System Architecture from College of Computer Science of the Xidian University, China, in 2013. Now he is a M.E. supervisor in the College of Computer and Cyber Security at the Fujian Normal University, Fuzhou, China. His research interests include mobile cloud computing systems, blockchain, and network security. He has published more than 50 papers in international journals and conferences.

Quanwen He graduated from College of Computer Science and Engineering at Chongqing University of Technology in 2020, he is a master student with the College of Computer and Cyber Security at the Fujian Normal University, Fuzhou, China. His main research interests include blockchain and access control.

Jia Hu is a Senior Lecturer in Computer Science at the University of Exeter. He received his PhD in Computer Science from the University of Bradford, UK, in 2010, and M.Eng. and B.Eng degrees in Electronic Engineering from Huazhong University of Science and Technology, Wuhan, China, in 2006 and 2004, respectively. His research interests include edge-cloud computing, resource optimization, applied machine learning, and network security. He has published over 100 research papers within these areas in prestigious international journals and reputable international conferences. He serves on the editorial board of Elsevier Computers & Electrical Engineering and has guest-edited many special issues on major international journals (e.g., IEEE IoT journal, Computer Networks, Ad Hoc Networks). He has served as General Co-Chair of IEEE CIT'15, IUCC'21, and Program Co-Chair of IEEE ISPA'20, ScalCom'19, SmartCity'18, CYBCONF'17, EAI SmartGIFT'2016, etc. He has received the Best Paper Awards at IEEE SOSE'16 and IUCC'14.

Xiaoding Wang received his Ph.D. in College of Mathematics and Informatics from Fujian Normal University in 2016, he is an Associate Professor with the College of Computer and Cyber Security at the Fujian Normal University, Fuzhou, China. His main research interests include network optimization and fault tolerance.