Heliyon 10 (2024) e23575

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Research article

Dual blockchain-based data sharing mechanism with privacy protection for medical internet of things

Linchen Liu [a], Ruyan Liu [b], Zhiying Lv [b], Ding Huang [b], Xing Liu [c,*]

[a] Department of Rheumatology, Zhongda Hospital, School of Medicine, Southeast University, 210009, Nanjing, Jiangsu, China
[b] Engineering Research Center of Digital Forensics of Ministry of Education, School of Computer Science, Nanjing University of Information Science and Technology, 210044, Nanjing, Jiangsu, China
[c] School of Medicine, Southeast University, 210009, Nanjing, Jiangsu, China

ARTICLE INFO

Keywords:
Medical internet of things
Medical data sharing
Blockchain
Privacy protection

ABSTRACT

In the period of big data, the Medical Internet of Things (MIoT) serves as a critical technology for modern medical data collection. Through medical devices and sensors, it enables real-time collection of a large amount of patients' physiological parameters and health data. However, these data are often generated in a high-speed, large-scale, and diverse manner, requiring integration with traditional medical systems, which further exacerbates the phenomenon of scattered and heterogeneous medical data. Additionally, the privacy and security requirements for the devices and sensor data involved in the MIoT are more stringent. Therefore, when designing a medical data sharing mechanism, the data privacy protection capability of the mechanism must be fully considered. This paper proposes an alliance chain medical data sharing mechanism based on a dual-chain structure to achieve secure sharing of medical data among entities such as medical institutions, research institutions, and cloud privacy centers, and at the same time provide privacy protection functions to achieve a balanced combination of privacy protection capability and data accessibility of medical data. First, a knowledge technology based on ciphertext policy attribute encryption with zero-knowledge concise non-interactive argumentation is used, combined with the data sharing structure of the federation chain, to ensure the integrity and privacy-protecting capability of medical data. Second, the approach employs certificate-based signing and proxy re-encryption technology, ensuring that entities can decrypt and verify medical data at the cloud privacy center using this methodology, consequently addressing the confidentiality concerns surrounding medical data. Third, an efficient and secure key identity-based encryption protocol is used to ensure the legitimacy of user identity and improve the security of medical data. Finally, the theoretical and practical performance analysis proves that the mechanism is feasible and efficient compared with other existing mechanisms.

1. Introduction

With technological innovation and social development, medical data is experiencing explosive growth. Effective management of medical data is crucial for researching new technologies and therapies for treating diseases, as well as improving the capability to

* Corresponding author.
E-mail addresses: llchen2023728@163.com (L. Liu), lry199903222937@163.com (R. Liu), nslvzy@foxmail.com (Z. Lv), hdfinder@163.com (D. Huang), 101006470@seu.edu.cn (X. Liu).

https://doi.org/10.1016/j.heliyon.2023.e23575
Received 18 August 2023; Received in revised form 2 December 2023; Accepted 6 December 2023

Available online 9 December 2023

identify public health risks and the standard of public medical services. In the modern medical field, the Medical Internet of Things (MIoT) [1] plays a significant role in technological innovation. By connecting medical devices and sensors to the internet, it enables real-time collection, transmission, and recording of medical data. These devices and sensors can monitor patients' physiological parameters, health status, and crucial data during the treatment process, providing valuable information resources for medical research and clinical practice, supporting personalized medicine and real-time monitoring services [2].

However, the rapid development of MIoT technology also brings new challenges to medical data management [3]. The intelligent nature of medical devices in MIoT enables them to connect to the internet and collect, transmit, and record patients' physiological parameters and health data in real-time [4]. The widespread adoption of smart medical devices makes data acquisition more convenient and offers new possibilities for medical and healthcare services. Yet, the high-speed, large-scale, and diverse nature of data generated by numerous devices and sensors involved in MIoT presents increased complexity in traditional medical data management. Data from different medical devices and sensors may have varying standards and formats, leading to further scattering and heterogeneity of medical data. Moreover, the stringent privacy and security requirements for the data from MIoT devices and sensors demand confidentiality and integrity to prevent data leakage and tampering. These new medical technologies and requirements have made medical data management more challenging [5].

The traditional approach to managing medical information involves centralized storage, a practice that is prone to issues such as loss of important medical data and invasion of personal privacy. As an open distributed ledger, blockchain technology provides the possibility of reshaping the management of medical data. Although blockchain has technical advantages such as transaction traceability, openness and transparency [6,7], and anonymity of user addresses, criminals can still analyze and infer their real private data through these anonymous addresses. Therefore, blockchain technology has insufficient privacy protection capability for sensitive data.

The security and privacy protection capabilities of medical data are prior options in the process of medical data management [8,9]. In order to make up for the lack of privacy protection of sensitive data by blockchain technology, this paper designs a consortium blockchain medical data sharing mechanism based on dual chain structure. The certificate based signcryption with proxy re-encryption (CBSRE) technology is introduced to meet the needs of medical data security and multi-user data access, and achieve the balance between the privacy protection capability and accessibility of medical data. In the process of medical data sharing, the CBSRE technology is used to decrypt the intermediate ciphertext encrypted by cloud privacy centers (CPC) to ensure the confidentiality of medical data. The efficient and secure key issuing identity-based encryption (ESKI-IBE) protocol [10] is introduced to improve the security of intermediate ciphertext and reduce the computation and communication costs of decrypting intermediate ciphertext. Among them, a single semi trusted key generation center (KGC) is responsible for user authentication during data management, and CPC is responsible for storing medical data and distributing private keys. In order to consider the privacy protection and security sharing of medical data in the whole process, the zero knowledge succinct non-interactive argument of knowledge (ZK-SNARK) technology based on ciphertext policy attributed-based encryption (CP-ABE) is used to realize the anonymity and privacy protection of medical data in the process of medical data sharing, and to solve the problem of data availability and fine-grained access control with consistent supply and demand. Meanwhile, smart contract (SC) can realize distributed consensus and automatic management of medical data security sharing [11]. Finally, from the theoretical analysis and practical performance analysis, the proposed mechanism is proved to have better privacy protection and execution efficiency than other existing mechanisms.

The main contributions of this paper are as follows:

- Dual-Chain Structure: We propose a novel dual-chain structure for medical data sharing, ensuring data integrity and addressing confidentiality concerns across various entities, including medical institutions and cloud privacy centers.
- Enhanced Privacy Protection: Our mechanism stands out by offering an unparalleled level of privacy protection for sensitive medical data in the MIoT landscape.
- Performance Analysis: Through meticulous testing, we showcase the superior efficiency and effectiveness of our mechanism, particularly in real-time medical data management scenarios.
- Comparative Analysis: We present a thorough comparison with existing solutions, underscoring the unique advantages and innovations brought forth by our approach.

The next part of this paper is organized as follows. Section 2, introduces the related work; Section 3, constructs the framework of the consortium blockchain medical data management mechanism based on the dual-chain structure; Section 4, constructs the dual-chain medical data management mechanism based on the dual-chain structure; Section 5, analyzes its theoretical and practical performance and compares it with the previous mechanisms; and Section 6, is the conclusion of this paper.

2. Related work

In this section, we introduce blockchain and the use of blockchain to solve data management problems in healthcare systems.

2.1. Blockchain

Blockchain, at its core, is a digital ledger system. Unlike traditional databases that rely on a central authority, blockchain is decentralized, distributing its information across multiple computers [12,13]. This decentralized nature ensures that no single entity holds excessive power over the entire chain, making tampering or unauthorized changes extremely challenging.

In traditional healthcare systems, a patient's data is stored in centralized databases, sometimes leading to data breaches, loss, or unauthorized access. Blockchain technology, with its tamper-resistant design, addresses this issue head-on. Every piece of data, once recorded on the blockchain, is virtually immutable. Any attempt to change a data block requires the consensus of the majority of participants in the network, ensuring that records remain pristine and unchanged [14,15].

Transparency is another hallmark of blockchain. All participants in a blockchain network can view transactions. Yet, in contrast, blockchain ensures the anonymity of its users. While transaction data is transparent, the identities of those involved in transactions are encrypted, offering a blend of open accountability and privacy.

Furthermore, the convergence of blockchain with Medical Internet of Things (MIoT) is ushering in a new era for healthcare [16]. MIoT refers to interconnected devices and sensors in the medical field. These tools can continuously monitor, collect, and send patient data. By integrating MIoT with blockchain, there's an assurance that this data is stored securely and remains unaltered [17,18]. For instance, a heart monitor connected to a patient might relay data to a blockchain. This data, once on the blockchain, becomes a part of the patient's immutable record, ensuring that doctors and medical professionals access only the most accurate and unaltered information.

The importance of such advancements cannot be understated, especially in a world where remote monitoring and telemedicine are becoming the norm. Patients and healthcare professionals can now trust the data's integrity they rely on for diagnoses, treatments, and ongoing care [19].

Moreover, research establishments benefit immensely from this technology [20]. With expedited and secure access to medical data, the research process is streamlined. Studies can be conducted faster, and the authenticity of the data used ensures more accurate outcomes [21].

In conclusion, while blockchain's intricate technicalities might seem overwhelming, its implications in healthcare are profoundly straightforward: a future where medical data is secure, transparent, accessible, and trustworthy. This not only revolutionizes how we view medical data management but also paves the way for a more efficient and reliable healthcare system globally.

2.2. Using blockchain to solve data management problems in medical systems

In the context of a blockchain-driven medical data management framework, pivotal considerations revolve around the efficacy of privacy protection and consensus establishment for medical data [22]. Omar and colleagues devised a patient-centric approach within blockchain-based medical data management, ensuring the confidentiality and security of patient-centric information [23]. A distinct proposition by Xia et al. addresses the sharing of medical data within a non-trusted environment, harnessing blockchain's capabilities to ensure the secure exchange of electronic medical records. Chen et al., on the other hand, introduced a hospital-centric private blockchain for medical data sharing and protection, establishing a dependable mechanism for archival and patient data retrieval [24]. In essence, these mechanisms integrate blockchain technology into the medical data management landscape, propelling advancements within the healthcare sector. Nevertheless, challenges persist in protecting medical data privacy, particularly in terms of its comprehensiveness and data accessibility across entities.

3. Medical data management mechanism framework of consortium blockchain based on dual chain structure

In this section, we introduce the concept of privacy data protection within the medical blockchain. We also present a framework for medical data management in a consortium blockchain, which is based on a dual-chain structure.

3.1. Privacy data protection in the medical blockchain

In the era of big data, MIoT technology enables real-time collection and transmission of medical data through sensors, devices, and internet connectivity, connecting medical equipment, medical instruments, and patient devices. Such real-time data collection and transmission provide more accurate and comprehensive data support for medical data management. Additionally, through MIoT technology, medical data can be conveniently integrated into the blockchain system, enabling real-time recording and storage of data [25]. However, the exposure of sensitive medical information (including patient details, medical procedures, and historical records) to the online sphere renders it susceptible to malicious attacks. For example, data leakage, data theft, malware infection, medical device attack and malware implantation. In the domain of medical data administration, compensating for the inherent privacy limitations of blockchain, this study devises a medical data management system that pivots on ensuring privacy protection and secure sharing of medical data. The focal aim centers on augmenting the management efficiency of medical data between healthcare establishments and research entities, fostering coherence between data supply and demand. In this framework, a privacy-enhanced consortium blockchain data sharing model [26,27] is employed to achieve precise access control over sensitive medical data and the confidentiality of access policies, thereby preventing unauthorized access and social engineering attacks. The Cloud Privacy Center (CPC) serves as the repository for medical data, accessible by multiple authorized entities through CPC. Additionally, CBSRE [28] technology and ESKI-IBE protocol ensure the integrity and confidentiality of medical data within CPC, making it less susceptible to data leakage, data theft, or malicious software attacks. ZK-SNARK technology is utilized to achieve anonymity and privacy protection of medical data, thus preventing data leaks and medical device attacks. Furthermore, a novel user private key generation method enhances the security of medical data within CPC, addressing potential user breaches in the key escrow and private key generation process.

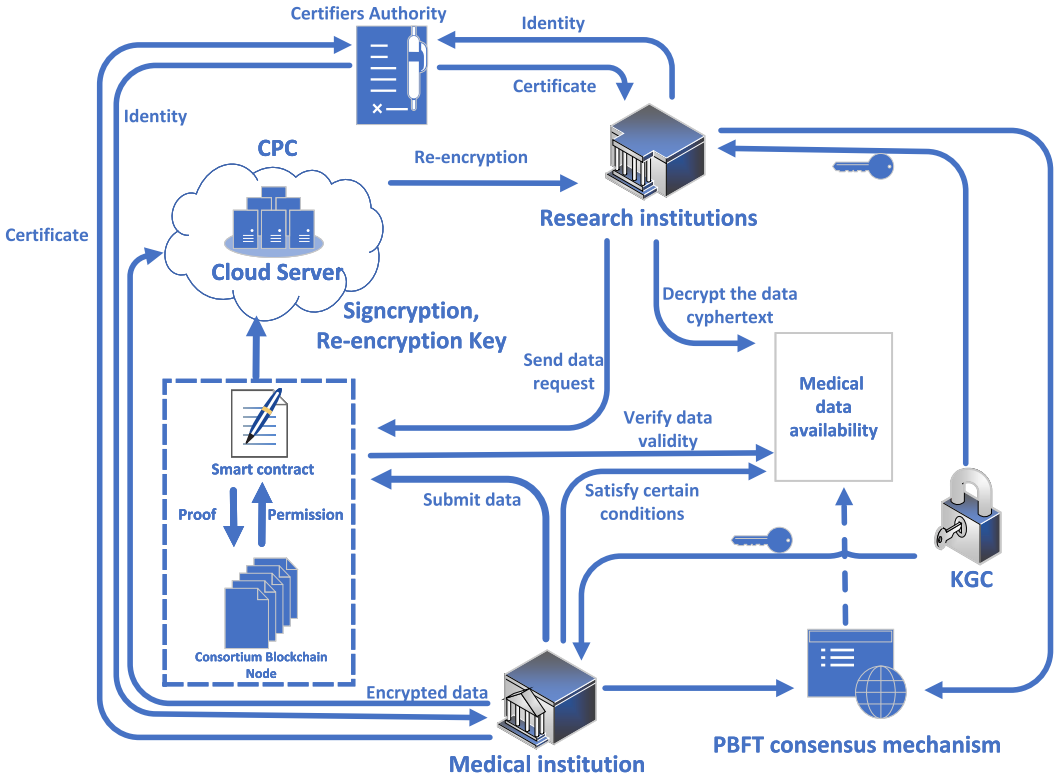

Fig. 1. Framework of medical data management mechanism of consortium blockchain based on dual chain structure.

3.2. *Framework of medical data management mechanism of consortium blockchain based on dual chain structure*

As shown in Fig. 1, the mechanism framework involves 7 entities: medical institutions, research institutions, KGC, CPC, consortium blockchain, SC, and Certification Authority (CA). Medical institutions and research institutions: as medical data management institutions, they need to be responsible for the security of patients' medical data. At the same time, a large amount of medical data is outsourced to CPC. For scientific research or other needs, when the medical data management institution needs to access the relevant medical data, it can issue the required medical data on the SC. The availability and validity of medical data is determined by the SC itself.

KGC: KGC is completely trusted, and there is no malicious operation. It authenticates the distributed entity institution, and distributes part of private keys to the entity institution [29]. Compared with the private key generator, KGC can prevent the abuse of the private keys of malicious users and improve the security of private keys of medical data. At the same time, the computation and communication overhead in the private key distribution process is reduced [30].

CA: The CA controls the registration process by generating certificates for SC through the identities of medical institutions and research institutions. SC ensures the secure transmission of medical data to the cloud server in CPC through signcryption technology. In this process, the security of the medical data stored by the CPC will be guaranteed.

CPC: Within the framework of the Medical Data Management Mechanisms based on a dual-chain structure, CPC plays a pivotal role. Not only is the CPC responsible for storing patient data supplied by various entities, but it also optimizes computing costs during cloud data storage [31]. Importantly, the CPC utilizes its own keys to protect the private keys of medical data, significantly enhancing data security. By seamlessly integrating with the dual-chain structure, the CPC ensures data security, accessibility, and transactability, all while preserving the privacy of patient data.

Consortium blockchain network: Each node's medical data index pointer, denoted as H_1, is subjected to CP-ABE encryption, fortifying the security and dependability of medical data. Furthermore, based on the PBFT consensus mechanism, all nodes on the consortium blockchain can verify and check ZK-SNARK parameters to guarantee the authenticity of medical data. Therefore, this mechanism can effectively break the problem of data lonely islands and prevent malicious nodes from accessing medical data information from the source, avoiding the risk of data leakage.

SC: Without the participation of a third party, the required institutions issue relevant data requirements to the SC to determine the exact demand for medical data. The SC automatically generates ZK-SNARK parameters and attributes of the medical data. During medical data sharing, the access policy of the medical data index attributes is always protected [32].

In this mechanism, the entity institutions upload medical data to a cloud server using signature encryption technology. At the same time, the index pointer of relevant medical data is stored in the SC to facilitate the subsequent management of medical data. If

Table 1
Meaning of symbols used in formulas.

re-encryption keys	$\mathcal{RK}_{s\mapsto r}$
ciphertext	φ
intermediate ciphertext	ϕ
safety parameter	λ
prime number	q
additive group	G_1
multiplicative group	G_2
hash functions	$H_1 : \{0,1\}^* \rightarrow G_1$
primary key	s_0
public key	P_i
blind factor	$x \in Z_q^*$
original private key	S_{ID}
sender certificate	C_s
generating element	P
two generalized elliptic curve divisor	D
shared public key	Y
receive parameters	D_0, X_0
private key	ϑ
receiver identity	ID_r
medical data	D
data attributes	$\mathbf{U}$, $\mathbf{PK_z}$, $\mathbf{VK_z}$
access policy	l
signcryption ciphertext	C
recelver certificate	C_r

the required institutions need corresponding medical data, they will send relevant requirements to the SC. In the sharing process, ZK-SNARK parameters and attributes of the medical data are automatically generated, and then automatically judged in the ZK-SNARK based SC. The validity of the judgment results directly determines the availability of data with consistent supply and demand. Once the verification is passed, the consortium blockchain gets the index pointer of the relevant medical data and connect it to CPC, and CPC checks it against the index pointer of the medical data and the index pointer of the medical data of CPC. If the comparison is successful, the CPC will use the 'ESKI-IBE protocol' to convert the encrypted medical data into an intermediate ciphertext, ensuring the integrity and privacy of the data. Subsequently, this intermediate ciphertext is transmitted to the required institutions to receive the signed medical data for the required institutions. After verifying the data availability of the received signature data, the desired data can be obtained. In this way, the required institutions can decrypt the plaintext using the private keys provided by the CPC to complete the automatic sharing of data. For the consideration of authority or commercial interests, every medical data sharing behavior on the consortium blockchain will be distributed consensus and finally recorded on the consortium blockchain.

4. Medical data management based on dual blockchain

In this section, we will delve into the details of medical data management based on a dual blockchain. We will cover the specific mechanism, the key issuing mechanism related to medical data security, the medical data security sharing mechanism based on CPC and consortium blockchain, the privacy protection mechanism of medical data using CPC and blockchain, as well as re-encryption, decryption, and the consensus stage. Table 1 indicates the meaning of the symbols used in the formula.

4.1. Specific mechanism

In this mechanism, medical data is encrypted with signcryption ciphertext φ and sent to the cloud server in CPC. At the same time, the index pointer H_1 of the data D is saved on the consortium blockchain. According to relevant requirements, when the required institutions need to use medical data, they will issue relevant requirements to the SC.

On the premise of meeting the security requirements, ZK-SNARK public parameter list and CP-ABE public parameter list need to be generated when the required institutions obtain the required medical data. The former is used to generate corresponding circuits. The latter is used to encrypt the attributes of medical data. The $Genproof$ algorithm is executed to generate a trusted zero-knowledge proof, and then the $Verproof$ algorithm is executed to verify that the provided medical data meets the requirements of the entity institutions.

If the verification of zero knowledge proof is successful, the SC will notify the required institutions and provide the medical data index pointer H_1. The medical data index pointer $H_1{}'$ in CPC is compared with the medical data index pointer on the consortium blockchain. If the comparison is successful, the signed medical data will be sent to CPC. That is, the required institutions generate the re-encryption keys $\mathcal{RK}_{s\mapsto r}$ (the conversion keys). The re-encryption keys $\mathcal{RK}_{s\mapsto r}$ is then sent to the CPC, where $\mathcal{RK}_{s\mapsto r}$ is encrypted by the public keys in CPC. CPC decrypts the re-encryption keys $\mathcal{RK}_{s\mapsto r}$ and executes the re-encryption algorithm, converting the ciphertext φ into an intermediate ciphertext ϕ that the desired institution can decrypt, and CPC then sends the ciphertext ϕ to the desired institution.

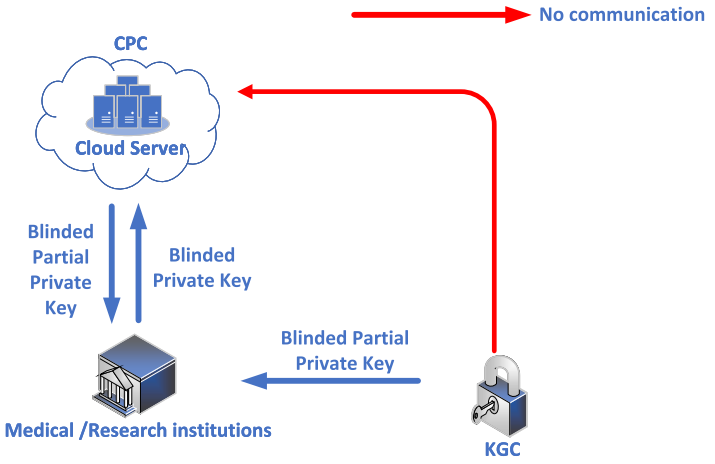

Fig. 2. Key issuing mechanism based on medical management system.

The required institutions verify whether Υ is equal to $\mathcal{Z}.D + (h_3(\mathcal{W}, \Upsilon, C)).(S_{ID}.D)$, and then computes and obtains medical data D. During this process, the CPC cannot retrieve any information related to the plaintext. Finally, the consortium blockchain submits the data sharing behavior to the verification nodes. This behavior documents the data sharing message between medical institutions and science organisations and issues it to the consortium blockchain after it is verified by the PBFT consensus algorithm.

4.2. Key issuing mechanism based on medical data security

The traditional public key cryptosystem (PKC) has the problems of key trusteeship and abuse. It requires a lot of memory and computing cost to manage digital certificates and revoke keys. Therefore, this mechanism uses KGC and CPC to solve key trusteeship, user defamation and other problems. KGC is responsible for verifying the identity of the user and distributing part of the entity private keys, and the CPC is responsible for securing private keys of the entity institutions. Fig. 2 illustrates the key issuing mechanism based on the medical management system.

Using the traditional public key cryptosystem to manage the relationship between the authentication authority and the user will result in a large amount of memory and communication overhead waste. Although PKC is trustworthy, it also has the problem of malicious distribution of private keys. Therefore, the mechanism uses the mechanism of generating user private keys to reduce the trust of a single private key generator, and reduce the private key computation cost and communication cost in medical data management. Meanwhile, the mechanism of generating user private keys can resist the attacks of the independence under hypothesis text attachment model for IBE (IND-ID-CCA) of the Bilinear Diffie Hellman Assumption, and improve the security of the medical data sharing process.

The user private key generation mechanism consists of the CPC and the KGC. When the required institutions request the private keys of medical data from KGC and CPC, KGC automatically verifies the legitimacy of identity of the required institutions. After the verification is passed, KGC will issue part of the private keys for storing the medical data to the required institutions, and CPC will send the rest of the private keys for medical data.

KGC inputs safety parameter λ, and λ-bit prime number q. Select an additive group G_1 and a multiplicative group G_2 of order q. Where, P is the generating element of G_1. Set $e : G_1 \times G_1 \to G_2$, hash functions $H_1 : \{0,1\}^* \to G_1$, and primary key $s_0 \in Z_q^*$. After that, output the public parameter $Param = q, e, P, P_0, G_1, G_2, H_1, Y, P_1, \cdots, P_n$ and the primary key s_0, where Y is the public key of the medical data. For key $s_i \in Z_q^*$ of each CPC^i, compute public key P_i of CPC and primary key s_0 as input, output their respective public key Y_i of the medical data, and then combine them to be the public key $Y = Y_n = s_n s_{n-1} \cdots s_0 P$ of the medical data and send them to KGC.

Give an ID as a unique identifier for the medical data. Select the blind factor $x \in Z_q^*$, and the KGC verifies the legitimacy of the requester's identity along with other receive parameters D_0, X_0 and sends them to the requester. The requester sends $\{ID, D_{i-1}, X_{i-1}\}$ to $CPC_i\,(i = 1, 2, \cdots, n)$, for requesting of ensuring private key protection of CPC^i, wherein, $1 \le i \le n$. Finally, the original private key $S_{ID} = x^{-1} D_n = s_0 s_1 \cdots Q_{ID}$ of medical data and the shared public key $Y = s_0 s_1 \cdots s_n P$ of medical data are obtained. Select the degenerate quadratic hyperelliptic curve ($\mathcal{HC}$), 80-bit keys and parameter size. D is the two generalized elliptic curve divisor, select h_0, h_1, h_2, h_3, h_4 with the functional nature of SHA512. ϑ is the private key of the primary key s_0, and $c = 2^{80}$. Finally, compute $\mathfrak{O} = (H\mathcal{C}, h_0, h_1, h_2, h_3, h_4, c, Z_c, P_0)$, and $\mathfrak{O}$ is common parameter set.

Select $\delta \in Z_c$, and since the complete public key $Y = s_0 s_1 \cdots s_n P$ of the entity institution and the complete private key $S_{ID} = x^{-1} D_n = s_0 s_1 \cdots Q_{ID}$ of the medical data have been generated, we can directly generate the certificate $C = \delta + \vartheta h_0(Y, S_{ID} \cdot D)$. Create signcryption ciphertext $\psi = (C_s, \mathcal{G}, \mathcal{Z})$, where C_s is the sender certificate. Compute $\mathcal{W} = k.D$, where $k \in Z_c$. Select $\eta \in \{0,1\}^{\Upsilon}$, provide the sender's ID_s, $massage(D)$ and receiver identity ID_r, and compute $\dagger = h_1(\eta, ID_s, m), \Upsilon = \dagger.D, \mathcal{Q}_s = Y + h_0(ID_s, \mathcal{FP}\beta_s).P_0$, where $\mathcal{FP}\beta_s$ is the public key of ID_s. Finally, the ciphertext $C = (\eta, ID_s, m) \oplus h_2(\dagger.\mathcal{Q}_s)$ is generated. Compute $\mathcal{G} = h_3(\mathcal{W}, \Upsilon, C), Z = \dagger - \mathcal{G}.Pk_s$, where Pk_s is the private key of ID_s. The computation formula of the final signcryption ciphertext is: $\psi = (C, \Upsilon, \mathcal{W}, \mathcal{Z})$.

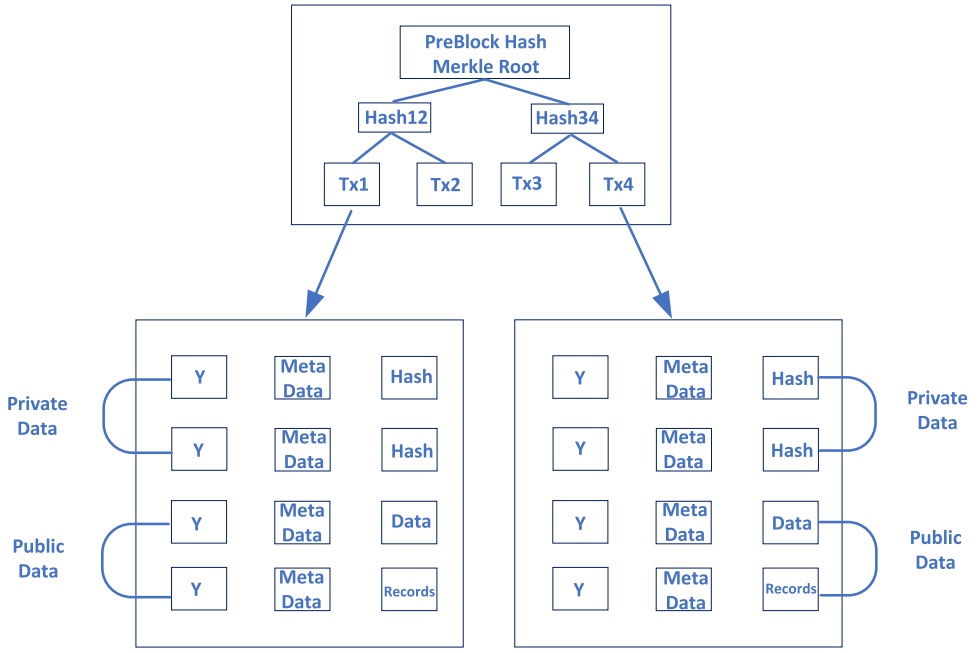

Fig. 3. Internal storage details of the consortium blockchain network.

In this mechanism, the consortium blockchain is divided into SC layer, network layer and data layer. After encryption, the medical data index pointer H_1 and attributes will be put into the data layer, and the medical data details will be uploaded to the cloud server in CPC for storage as signcryption ciphertext ψ. The index pointer H_1 and attributes of medical data are stored on the consortium blockchain to generate the transaction table shown in Fig. 3. After the required institutions submit the access requirement, the consortium blockchain generates a SC for the ZK-SNARK parameters and attributes of the medical data. Assuming that the data is shared successfully, the access policy and access record are saved on the consortium blockchain through the distributed consensus PBFT mechanism. Meanwhile, based on CP-ABE mechanism, all sensitive attributes of shared data index pointers and data keywords will be protected.

$$\dagger = h_1\left(\eta, ID_s, m\right), \Upsilon = \dagger \cdot \mathcal{D}, \mathcal{Q}_s = Y + h_0\left(ID_s, \mathcal{FP}\beta_s\right) \cdot P_0 \tag{1}$$

4.3. Medical data security sharing mechanism based on CPC and consortium blockchain

As shown in Fig. 4, the required institutions automatically identify and extract the relevant medical data index pointer H_1 and the attributes of the data on the consortium blockchain according to the data requirements issued by them. At the same time, all access information and access policies will be recorded on the consortium blockchain network.

The SC layer is composed of ZK-SNARK SC and CP-ABE SC. Therefore, the consortium blockchain adopts the dual chain structure. The former is used to generate zero-knowledge verification parameters from the access policy submitted by the user nodes and verify the zero-knowledge proof parameters submitted by the nodes. After the current one passes the verification, the latter submits the attributes to it, and finally returns the decryption keys of attributes through the secure channel for decryption.

If the required institutions want to obtain medical data, after sending the request, the consortium blockchain generates ZK-SNARK SC, and uses its own attributes to generate CP-ABE SC. After the validity of medical data is verified by the SC layer, the index pointer H_1 of the medical data and the attributes of the data are obtained. Then, the medical data index pointer H_1 on the consortium blockchain is compared with the medical data index pointer H_1' in CPC. If the comparison is successful, the specific data is re-encrypted for the required institutions and sent to these institutions. After receiving the signed data and verifying the availability of the data against the signed data received, the CPC distributes the private keys of the medical data to the required institutions. Finally, the required institutions use the private keys of the medical data provided by the CPC to get the specified shared data.

4.4. Privacy protection mechanism of medical data based on CPC and blockchain

In the process of encrypting medical data submitted to the consortium blockchain using ZK-SNARK zero-knowledge proofs, we first initiate a one-time setup to generate a common reference string. After defining the medical data, we create a proof that conceals the original data. This encrypted data, along with its proof, is then submitted to the consortium blockchain. Any participant of the

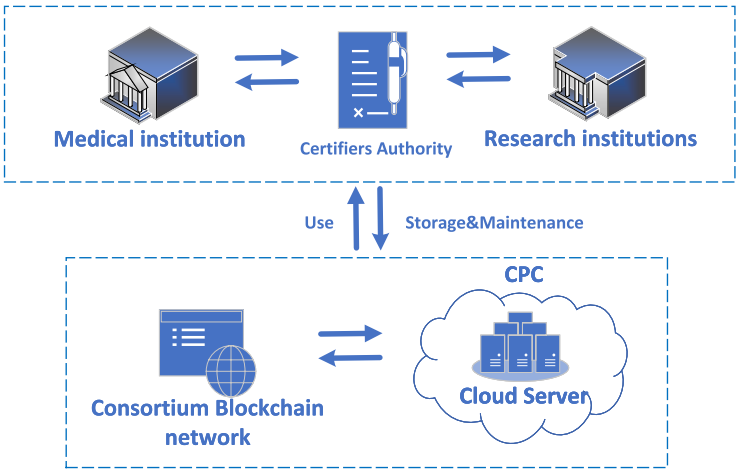

Fig. 4. Framework of medical data security sharing based on cloud privacy centers and blockchain.

consortium blockchain can use these public parameters to verify the authenticity of the data without accessing the original data. Upon verification, the ZK-SNARK parameters are integrated into the data layer, ensuring both the privacy and integrity of the data.

When smart devices in the MIoT collect medical data, the entity institutions submit the medical data to the consortium blockchain. The consortium blockchain will automatically generate SC based on the attributes of the medical data. At the same time, the consortium blockchain encrypts the index pointer H_1 of medical data, puts it into the data layer of the consortium blockchain and automatically generates ZK-SNARK parameters. When the required institutions want to obtain the medical data stored in the cloud server of CPC, the consortium blockchain automatically obtains the information and generates the ZK-SNARK parameters and attributes after issuing relevant requirements to the blockchain. When the attributes and ZK-SNARK parameters of the medical data required for verification are consistent with the relevant data on the consortium blockchain, the consortium blockchain provides the index pointer H_1 to the required institutions. The required institutions check against the index pointer H_1 and the index pointer H_1' for medical data in CPC. If the comparison is successful, the CPC will distribute the private keys of medical data to the required institutions. The required institutions access medical data from cloud server in CPC, and integrate access records and access policies into the entire consortium blockchain through a distributed consensus PBFT mechanism.

In the whole process, the attributes of the stored medical data and the access policy of the required medical data are protected. At the same time, no node on the blockchain knows the sensitive attributes of the medical data, because it only submits the proof of the data attributes to the consortium blockchain, and everyone can verify it. The access policy is used to encrypt data.

First of all, ZK-SNARK SC and CP-ABE SC were initialized in combination with [26] to establish a consortium blockchain with dual chain structure. The CP-ABE SC generates the primary key $\mathbf{MK} = (\beta, g^a)$ when the medical data is on the blockchain and encrypted using an access policy. After the primary key $\mathbf{MK}$ is generated, the public key $Y_b = G_1, g, h = g^\beta, f = g^{1/\beta}, (g,g)^a$ is automatically generated and the selection key $\left(O = g^{\frac{a+r}{\beta}}, \forall j \in S : O_j = g^r \cdot H(j)^{r_j}, O_j' = g^{r_j}\right) \rightarrow S_{ID}$ is generated. When the required institutions make a data request to the consortium chain, the ZK-SNARK parameters are generated on the blockchain. At the same time, the ZK-SNARK SC layer uses the verification keys to verify the ZK-SNAR parameters and automatically generate $\mathbf{PK_z}$ and $\mathbf{VK_z}$. If the ZK-SNARK SC layer verifies that the ZK-SNARK parameters are valid, the entity institutions will obtain the decryption keys used to decrypt the encrypted medical data index pointer H_1.

In order to achieve the above requirements, the required institutions use Algorithms 1 and 2 to input access policy and automatically generate ZK-SNARK parameters and transmit them to the SC layer. The required institutions obtain the ZK-SNARK parameters through the SC, generates the attributes U of the required medical data, and verifies the ZK-SNARK parameters automatically through Algorithm 3. If the verification is correct, the medical data index pointer H_1 is decrypted by Algorithm 4.

Generation of ZK-SNARK public parameters. The specific circuit is set as the input access policy to ensure that the attributes $\mathbf{U} = \{u_1, u_2, u_3, \cdots\}$ used for verification meets the requirements of the access policy, so that the corresponding circuit is automatically generated. Where, l is the access policy, $\mathbf{U}$, $\mathbf{PK_z}$, $\mathbf{VK_z}$ are as the data attributes.

Algorithm 1 ZK-SNARK smart contract setup.

Input: Access Policy, A security parameter λ
Output: ZK-SNARK public parameters $\mathbf{pp_z}$
1: $Setup(1^\lambda) \rightarrow \mathbf{pp_z}$
2: **For** each policy l in Access Policy:
3: Construct a circuit $C_l(D)$
4: $KeyGen(C_l(D)) \rightarrow (pk_z, vk_z)$
5: **Set** $\mathbf{PK_z} = \cup pk_z$ and $\mathbf{VK_z} = \cup vk_z$
6: **Output** $\mathbf{pp_z} = (\mathbf{PK_z}, \mathbf{VK_z})$

Generation of CP-ABE public parameter list. It is mainly used for encrypting attributes of medical data on the consortium blockchain.

Algorithm 2 CP-ABE smart contract setup.

Input: Access Control, A security parameter κ
Output: CP-ABE public parameters $\mathbf{pp_b}$
1: $Setup(1^{\kappa}) \rightarrow \mathbf{pp_b}$
2: **For** parameter $\mathbf{l}^{\kappa}$:
3: Compute $\mathbf{MK_b} = (\beta, g^a)$
4: Compute $Y_b = G_1, g, h = g^{\beta}, f = g^{1/\beta}, e(g,g)^a$
5: **Output** $\mathbf{pp_b} = (Y_b)$

Generation and verification of ZK-SNARK parameters. The attributes and ZK-SNARK parameters of the medical data input by the required institutions generate ZK-SNARK, and transmit it to the ZK-SNARK SC layer for verification. After the verification is passed, the required institutions will have access to the CP-ABE SC layer.

Algorithm 3 Proof generation and verification.

Input: Attributes $\mathbf{U}, \mathbf{PK_z}, \mathbf{VK_z}$
Output: Proof, Permission or Denial
1: **For** pk_z **in** $\mathbf{PK_z}$:
2: $Genproof(Attributes\ \mathbf{U}, pk_z) \rightarrow proof_z$
3: $\mathbf{Proof_z} = \cup proof_z$
4: **For** $proof_z$ in $\mathbf{Proof_z}$
5: Compute $Verproof(proof_z, vk_z)$
6: **If** $Verproof(proof_z, vk_z)$ succeed:
7: Give right to access CP-ABE Smart Contract
8: **If** $Verproof(proof_z, vk_z)$ fail:
9: Deny access request
10: **Output** Permission or Denial

Encryption and decryption of medical data. The entity institutions transmit the access policy to the CP-ABE SC layer, and the CP-ABE SC layer return the access policy that can be used to encrypt the attributes of medical data. After the ZK-SNARK SC layer verifies the ZK-SNARK parameters, the required institutions can submit the attributes $\mathbf{U}$ of medical data to the CP-ABE SC layer. S_{ID} acquired by the required institutions, used to decrypt the medical data index pointer H_1.

Algorithm 4 Data encryption and decryption.

Input: Access policy, Permission, Attributes $\mathbf{U}$, D
Output: Encrypted Data
1: **For** D, Y,Access policy :
2: $Encrypt(Y$,Access policy,$D) \rightarrow d$
3: **For** Permission, **MK** and Attributes $\mathbf{U}$:
4: $\left(O = g^{\frac{\alpha+r}{\beta}}, \forall j \in S : O_j = g^r \cdot H(j)^{r_j}, O'_j = g^{r_j}\right) \rightarrow S_{ID}$
5: **For** S_{ID} and Encrypted data:
6: $Decrypt(S_{ID}$,$Encypted\ D) \rightarrow D$
7: **Output** D

4.5. Re-encryption and decryption

Provide the sender certificate C_s, and the required institutions can obtain the conversion key $\mathcal{RK}_{s \mapsto r}$ after obtaining the medical data index pointer H_1. Compute $S = h_4(ID_s, ID_r, \mathcal{P}k_s(Y + h_0(ID_r, \mathcal{FP}\beta_r).P_0))$ and $\mathcal{RK}_{s \mapsto r} = \frac{Pk_s + C_s}{S}$. After that, send $\mathcal{RK}_{s \mapsto r}$ to CPC, and CPC first check whether Υ is equal to $\mathcal{Z}.D + (h_3(\mathcal{W}, \Upsilon, C)).(S_{ID}.D)$. Then set the secondary signcryption ciphertext $C^{/}$ of the intermediate ciphertext be equal to the primary signcryption ciphertext C, so that the required institutions can use the keys to decrypt. Finally, CPC sets the intermediate ciphertext $\phi = (C^{/}, \mathcal{RK}_{s \mapsto r}, \Upsilon, \mathcal{Z}, \mathcal{G})$ as a secondary ciphertext that is sent to the required institutions.

Give the receiver certificate C_r. If entity institutions need to decrypt the data they want, it needs to first verify whether Υ is equal to $\mathcal{Z}.D + (h_3(\mathcal{W}, \Upsilon, C)).(S_{ID}.D)$. If the verification is passed, compute $S^{/} = h_4(ID_r, ID_s(Pk_r + C_r)Y)$. Finally, the required institutions decrypt $(\eta, ID_s, FNs, D)^{/} = C^{/} \oplus h_2(S^{/}\mathcal{RK}_{s \mapsto r}\Upsilon)$ to obtain the required medical data index H'_1. If the comparison of H_1 and H'_1 is successful, CPC will distribute the private keys of medical data to the required institutions. Finally, the required institutions access the relevant medical data of the cloud server in CPC according to the private keys provided by CPC.

Table 2
Comparison of mainstream consensus algorithms.

Characteristic	Proof of Work (PoW)	Proof of Stack (PoS)	Delegated Proof of Stake (DPoS)	PBFT
Nodes Management	No Permission	No Permission	No Permission	Permission Required
Transaction Delay	High	Low	Low	Very Low
Throughput	Low	High	High	High
Energy Saving	No	Yes	Yes	Yes
Security Boundary	1/2 Malicious Computing Power	1/2 Malicious Stakes	1/2 Malicious Stakes	1/3 Malicious Nodes
Scalability	Good	Good	Good	Poor
Typical Application	Bitcoin	Peercoin	BitShares	Fabric

4.6. Consensus stage

In our proposed mechanism, we integrate the Practical Byzantine Fault Tolerance (PBFT) algorithm, a well-known consensus algorithm adept at dealing with system failures, including Byzantine failures. The adoption of PBFT improves the system reliability even in the presence of possible malicious or unpredictable behaviors of some nodes, which for healthcare data, where accuracy and reliability are critical, is indispensable. In addition to reliability, PBFT enables deterministic consensus in a relatively short period of time, ensuring timely processing of data, in contrast to other consensus algorithms that may result in lengthy communication rounds or provide only probabilistic guarantees. The inherent design of the PBFT algorithm strengthens the system's resilience against potential counterfeit attacks, ensuring that malicious nodes cannot easily take control of the network. By incorporating the PBFT algorithm into our mechanism, we ensure that the scheme in this paper has high reliability, efficiency, security, and scalability.

As shown in Table 2, mainstream algorithms are compared in terms of node management, mechanism construction and maintenance cost, and practicality. Finally, it is demonstrated that the PBFT algorithm is the most suitable choice for this system.

Therefore, after the required institutions decrypt the medical data obtained from the CPC, the Smart Contract (SC) submits the medical data sharing process to the verification nodes. These verification nodes, using the PBFT [33–35] consensus algorithm, rigorously examine the data sharing operation. The PBFT algorithm, chosen for its robustness and ability to withstand up to (n-1)/3 Byzantine nodes, ensures the correctness of the distributed consensus process even in the presence of malicious nodes. If verified, the SC will automatically publish the behavior and record it on the consortium blockchain.

5. System analysis

In this section, the analysis of the basic security requirements for confidentiality, integrity, validity and availability of medical data as well as the privacy protection capability will be illustrated from three aspects of security analysis. At the same time, the practicability of the mechanism is evaluated from the actual performance analysis.

5.1. Analysis on security

In this mechanism, all medical data will be encrypted using CBSRE technology in advance and uploaded to the cloud server in CPC, and the index pointer H_1' will be added to the medical data. At the same time, the SC also retains the index pointer H_1 of the medical data. This facilitates the search and security of medical data. Compared with traditional proxy encryption technology, the CBSRE technology can neither crack the ciphertext of medical data nor infer any information of the ciphertext from the inside or outside, ensuring the security and confidentiality of medical data.

The medical data existing in the entity institutions will generate the corresponding ZK-SNARK parameters through the SC on the consortium blockchain, and the ZK-SNARK SC layer will automatically generate the medical data index pointer H_1. At the same time, this behavior is conduced the distributed consensus by PBFT algorithm. As a kind of blockchain, consortium blockchain is also immutable, thus ensuring the integrity of medical data.

The required institutions shall check the index pointer H_1 according to the index pointer H_1' of medical data in CPC. If the comparison is successful, CPC will distribute the private keys of medical data to the required institutions. The required institutions access medical data from cloud servers in CPC, and the access records and policies are incorporated into the entire consortium blockchain network through the distributed consensus PBFT mechanism.

When the required institutions need to use the relevant medical data, the relevant requirements will be sent to the SC. The SC will verify whether this type of medical data exists and meets the use requirements of the required institutions through the medical data index pointer H_1 and ZK-SNARK parameters. If the match is successful, the required institutions will obtain the medical data index pointer H_1. After that, CPC verifies the availability of the medical data according to the index pointer H_1 and the index pointer H_1' in the cloud server. After the verification is passed, the medical number of the signcryption in the cloud server of CPC will be transmitted to the required institutions. Therefore, this function can effectively ensure the validity of data and the availability of consistent supply and demand.

Table 3
Comparison of system performance.

	Less computing cost	Fewer startup nodes	Privacy protection
MedRec(PoW)	False	False	False
ModelChain(PoI)	False	False	False
MDSM(DPoS)	True	False	True
This paper (PBFT)	True	True	True

5.2. Analysis of privacy protection capability

Within the framework of this consortium blockchain, there's an intrinsic mechanism that rigorously vets all participating entities, ensuring the authenticity and legitimacy of each participant. This not only provides a layer of trust but also establishes a barrier against potential infiltrators.

One of the standout features of this mechanism is its discerning approach to data sharing. Instead of sharing all data attributes, only specific, demanded attributes are made public. This selective approach is instrumental in mitigating the risks associated with data forgery, especially in the realm of medical data where accuracy is paramount.

On this blockchain, nodes representing legitimate entities operate with an unwavering commitment to the privacy of medical data. Their operations aren't in silos; every node within the system can verify and scrutinize data-sharing actions, ensuring transparency and adherence to established protocols.

The encryption technique, CP-ABE, employed on each node of this consortium blockchain, is noteworthy. It facilitates user access in accordance with predefined policy attributes. So, when a user with the right credentials seeks access, they can decrypt the medical data seamlessly. Every instance of data sharing is diligently recorded on the blockchain. Should any discrepancies or violations arise, the smart contract (SC) records can serve as an indisputable testament to the event, fortifying accountability.

In terms of access control, the mechanism is tailored to be fine-grained. It aligns with the nuanced requirements of data sharing, ensuring that sensitive medical data remains safeguarded and the risk of unwarranted exposure is drastically reduced.

Beyond these features, the underlying architecture of this mechanism is decentralized, built upon a dual-chain structure within the consortium blockchain. This design is purposeful, aiming to eradicate the vulnerabilities associated with a single point of failure. Every data sharing action undertaken by entity institutions is meticulously documented, bolstering transparency.

Lastly, the mechanism doesn't merely stop at protecting data. During the data-sharing processes on the consortium blockchain, it ensures that sensitive access policies and the unique attributes of critical data are shielded. This dual-layered approach not only secures the data but also the policies governing access to it, reinforcing the privacy and integrity of medical data.

In addition, this mechanism is a decentralized storage mechanism of consortium blockchain based on dual chain structure, which can effectively avoid the occurrence of single point of failure.

5.3. Performance analysis

This mechanism is compared with MedRec [36], ModelChain [37] and MeDShare [38] mechanisms, as shown in Table 3. The former two does not effectively protect the privacy of medical data. The MedRec mechanism provides a comprehensive personalized medical data management mechanism that solves the problems of fragmented medical data and slow data interaction. However, this mechanism uses the PoW consensus mechanism and requires a large number of blockchain nodes as support, resulting in low efficiency and other problems. The ModelChain mechanism combines machine learning with blockchain technology to solve the problem of healthcare predictive modeling tasks in data privacy protection and improve interoperability among entities. However, the mechanism uses the POI (Proof of Importance) consensus mechanism to require a large number of nodes, which affects the overall stability of the mechanism. The MeDShare is a mechanism for healthcare data management in an untrusted environment. In this mechanism, the risk of privacy disclosure of medical data is reduced. However, the DPoS consensus mechanism is used in the mechanism, ignoring the quantity of required blockchain nodes, increasing the workload of blockchain.

The block generation time, a critical metric for any blockchain mechanism, was a testament to our mechanism's efficiency. Under a Windows system with Intel(R) Core(TM) i7-3687U CPU @2.10GHz and 8GB RAM, our mechanism consistently outperformed its peers. The data from Fig. 5 reveals a compelling narrative: our mechanism not only generated blocks faster but also maintained a consistent performance, making it a reliable choice for real-time medical data management.

The efficiency of our zero-knowledge proofs was another highlight. We took a deep dive into the time metrics associated with the generation of proof key pairs (KeyGen), proving time (Prove time), and verification time (Verify). The results from 100 tests were not just consistent but also showcased our mechanism's superiority. The KeyGen time was significantly faster, and the Prove and Verify times were optimized for swift data transactions, ensuring that data integrity and privacy were maintained without compromising on speed.

A closer look at Fig. 5 provides more insights. The graph patterns and data points indicate that our mechanism's overhead is minimal, which is a significant advantage. In high transaction volume scenarios, this reduced overhead translates to faster data processing and sharing. This efficiency is paramount in real-time medical applications where timely data access can be crucial.

Furthermore, the experimental results also highlighted the adaptability of our mechanism. In varying load conditions and data volumes, the mechanism exhibited resilience and scalability, ensuring that performance did not degrade. This adaptability is crucial

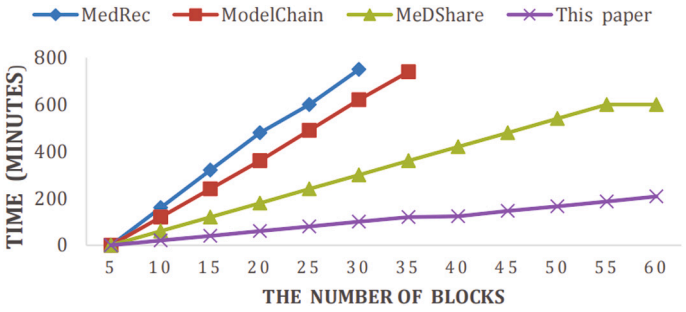

Fig. 5. Comparison of overhead under different mechanisms.

Table 4
Comparison between this mechanism and ADSNARK mechanism.

	ADSNARK	This paper
KeyGen	299 s	14 s
Prove	491 s	46 s
Verify	0.062 s	0.516 s
Proving key size	319 MB	14.7 MB
Verification key size	31 KB	105.3 KB

for real-world applications where data loads can be unpredictable. The granular details of our experimental results underscore the proposed mechanism's prowess in terms of efficiency, speed, and privacy protection. These results not only solidify our claims but also position our mechanism as a frontrunner for future innovations in medical data management.

Finally, this mechanism is compared with ADSNARK [39] mechanism in terms of KeyGen time of zero knowledge proof, time of KeyGen size and required time for Prove and Verify, as shown in Table 4.

6. Conclusions

By MIoT collects medical data through smart sensors and devices, making the acquisition and transmission of medical data easier and more efficient, and can make this data more useful in the healthcare field. However, due to its high sensitivity, it is vulnerable to attacks and misuse. In the design of medical data management mechanism, the privacy protection and secure sharing ability of medical data must be fully considered.

To address these concerns, we've introduced a blockchain data sharing model underpinned by CP-ABE, ensuring the safeguarding of medical data's sensitive attributes. Our innovative approach, which melds consortium blockchain, smart contracts, and ZK-SNARK technology, facilitates both medical data sharing and robust privacy protection among various entities. This synergy offers a fortified technical foundation for the secure exchange of medical data. Furthermore, the integration of CBSRE technology bolsters the storage security and veracity of medical data within the cloud privacy center. The ESKI-IBE protocol, on the other hand, vouches for the legitimacy of entity identities while optimizing computational and storage overheads associated with user private key generation. Complementing these, the PBFT consensus mechanism ensures comprehensive documentation of all medical data sharing activities. We culminate our paper with both theoretical and empirical performance analyses, underscoring the system's efficiency and viability.

In the future, the dynamic realm of MIoT and medical data management presents exciting opportunities for further research. The integration of advanced cryptographic techniques, exploration of quantum-resistant algorithms, and the quest for more efficient consensus algorithms or distributed storage solutions are potential avenues that can further elevate the security and scalability of medical data management systems in the future.

CRediT authorship contribution statement

Linchen Liu: Writing – review & editing, Writing – original draft, Validation, Methodology, Investigation, Formal analysis, Conceptualization. **Ruyan Liu:** Writing – original draft, Visualization, Validation, Software, Methodology, Formal analysis, Conceptualization. **Zhiying Lv:** Writing – review & editing, Visualization, Software, Investigation. **Ding Huang:** Writing – review & editing, Visualization, Software, Investigation. **Xing Liu:** Writing – review & editing, Supervision, Project administration, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The data that has been used is confidential.

Funding

This work was supported by the National Natural Science Foundation of China (Grant No. 62072249).

References

[1] N. Akhtar, S. Rahman, H. Sadia, Y. Perwej, A holistic analysis of medical internet of things (miot), J. Inf. Comput. Sci. 11 (4) (2021) 209–222.
[2] H. Elayan, R.M. Shubair, A. Kiourti, Wireless sensors for medical applications: current status and future challenges, in: 2017 11th European Conference on Antennas and Propagation (EUCAP), IEEE, 2017, pp. 2478–2482.
[3] M. Elhoseny, N.N. Thilakarathne, M.I. Alghamdi, R.K. Mahendran, A.A. Gardezi, H. Weerasinghe, A. Welhenge, Security and privacy issues in medical internet of things: overview, countermeasures, challenges and future directions, Sustainability 13 (21) (2021) 11645.
[4] D.V. Dimitrov, Medical internet of things and big data in healthcare, Healthc. Inform. Res. 22 (3) (2016) 156–163.
[5] B. Xu, L. Da Xu, H. Cai, C. Xie, J. Hu, F. Bu, Ubiquitous data accessing method in iot-based information system for emergency medical services, IEEE Trans. Ind. Inform. 10 (2) (2014) 1578–1586.
[6] Y. Ren, F. Zhu, P.K. Sharma, T. Wang, J. Wang, O. Alfarraj, A. Tolba, Data query mechanism based on hash computing power of blockchain in internet of things, Sensors 20 (1) (2019) 207.
[7] Y. Chen, S. Ding, Z. Xu, H. Zheng, S. Yang, Blockchain-based medical records secure storage and medical service framework, J. Med. Syst. 43 (2019) 1–9.
[8] A. Torfi, E.A. Fox, C.K. Reddy, Differentially private synthetic medical data generation using convolutional gans, Inf. Sci. 586 (2022) 485–500.
[9] F. Yu, H. Shen, Q. Yu, X. Kong, P.K. Sharma, S. Cai, Privacy protection of medical data based on multi-scroll memristive Hopfield neural network, IEEE Trans. Netw. Sci. Eng. 10 (2) (2022) 845–858.
[10] M. Kumar, S. Chand, Eski-ibe: efficient and secure key issuing identity-based encryption with cloud privacy centers, Multimed. Tools Appl. 78 (2019) 19753–19786.
[11] Y. Ren, D. Huang, W. Wang, X. Yu, Bsmd: a blockchain-based secure storage mechanism for big spatio-temporal data, Future Gener. Comput. Syst. 138 (2023) 328–338.
[12] P. Xi, X. Zhang, L. Wang, W. Liu, S. Peng, A review of blockchain-based secure sharing of healthcare data, Appl. Sci. 12 (15) (2022) 7912.
[13] J.-S. Lee, C.-J. Chew, J.-Y. Liu, Y.-C. Chen, K.-Y. Tsai, Medical blockchain: data sharing and privacy preserving of ehr based on smart contract, J. Inf. Secur. Appl. 65 (2022) 103117.
[14] G. Xu, C. Qi, W. Dong, L. Gong, S. Liu, S. Chen, J. Liu, X. Zheng, A privacy-preserving medical data sharing scheme based on blockchain, IEEE J. Biomed. Health Inform. 27 (2) (2022) 698–709.
[15] Y. Ren, Y. Leng, Y. Cheng, J. Wang, Secure data storage based on blockchain and coding in edge computing, Math. Biosci. Eng. 16 (4) (2019) 1874–1892.
[16] M. Dachyar, T.Y.M. Zagloel, L.R. Saragih, Knowledge growth and development: internet of things (iot) research, 2006–2018, Heliyon 5 (8) (2019).
[17] N. Mehta, A. Pandit, S. Shukla, Transforming healthcare with big data analytics and artificial intelligence: a systematic mapping study, J. Biomed. Inform. 100 (2019) 103311.
[18] C. Xie, P. Yang, Y. Yang, Open knowledge accessing method in iot-based hospital information system for medical record enrichment, IEEE Access 6 (2018) 15202–15211.
[19] K. Azbeg, O. Ouchetto, S. Andaloussi, L. Fetjah, A taxonomic review of the use of iot and blockchain in healthcare applications, IRBM 43 (5) (2022) 511–519.
[20] A. Priyanka, M. Parimala, K. Sudheer, R. Kaluri, K. Lakshmanna, M.P.K. Reddy, et al., Big Data Based on Healthcare Analysis Using Iot Devices, IOP Conference Series: Materials Science and Engineering, vol. 263, IOP Publishing, 2017, p. 042059.
[21] W.-C. Hsu, J.-H. Li, Visualising and mapping the intellectual structure of medical big data, J. Inf. Sci. 45 (2) (2019) 239–258.
[22] A. Farouk, A. Alahmadi, S. Ghose, A. Mashatan, Blockchain platform for industrial healthcare: vision and future opportunities, Comput. Commun. 154 (2020) 223–235.
[23] A. Al Omar, M.S. Rahman, A. Basu, S. Kiyomoto, Medibchain: a blockchain based privacy preserving platform for healthcare data, in: Security, Privacy, and Anonymity in Computation, Communication, and Storage: SpaCCS 2017 International Workshops, Guangzhou, China, December 12-15, 2017, Proceedings 10, Springer, 2017.
[24] Y. Chen, L. Meng, H. Zhou, G. Xue, A blockchain-based medical data sharing mechanism with attribute-based access control and privacy protection, Wirel. Commun. Mob. Comput. 2021 (2021) 1–12.
[25] H. Habibzadeh, K. Dinesh, O.R. Shishvan, A. Boggio-Dandry, G. Sharma, T. Soyata, A survey of healthcare internet of things (hiot): A clinical perspective, IEEE Int. Things J. 7 (1) (2019) 53–71.
[26] X. Shang, L. Tan, K. Yu, J. Zhang, K. Kaur, M.M. Hassan, Newton-interpolation-based zk-snark for artificial internet of things, Ad Hoc Netw. 123 (2021) 102656.
[27] Y. Ren, F. Zhu, J. Wang, P.K. Sharma, U. Ghosh, Novel vote scheme for decision-making feedback based on blockchain in internet of vehicles, IEEE Trans. Intell. Transp. Syst. 23 (2) (2021) 1639–1648.
[28] A. Braeken, P. Shabisha, A. Touhafi, K. Steenhaut, Pairing free and implicit certificate based signcryption scheme with proxy re-encryption for secure cloud data storage, in: 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), IEEE, 2017, pp. 1–7.
[29] Y. Ren, Y. Leng, J. Qi, P.K. Sharma, J. Wang, Z. Almakhadmeh, A. Tolba, Multiple cloud storage mechanism based on blockchain in smart homes, Future Gener. Comput. Syst. 115 (2021) 304–313.
[30] Q. Wu, Z. Han, G. Mohiuddin, Y. Ren, Distributed timestamp mechanism based on verifiable delay functions, Comput. Syst. Sci. Eng. 44 (2) (2023).
[31] J. Wang, J. Chen, Y. Ren, P.K. Sharma, O. Alfarraj, A. Tolba, Data security storage mechanism based on blockchain industrial internet of things, Comput. Ind. Eng. 164 (2022) 107903.
[32] X. Yu, S. Zhu, Y. Ren, Continuous trajectory similarity search with result diversification, Future Gener. Comput. Syst. 143 (2023) 392–400.
[33] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, M.A. Imran, A scalable multi-layer pbft consensus for blockchain, IEEE Trans. Parallel Distrib. Syst. 32 (5) (2020) 1146–1160.
[34] W. Viriyasitavat, L. Da Xu, Z. Bi, A. Sapsomboon, New blockchain-based architecture for service interoperations in internet of things, IEEE Trans. Comput. Soc. Syst. 6 (4) (2019) 739–748.
[35] J. Qu, Blockchain in medical informatics, J. Indust. Inf. Integr. 25 (2022) 100258.
[36] A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, Medrec: using blockchain for medical data access and permission management, in: 2016 2nd International Conference on Open and Big Data (OBD), IEEE, 2016, pp. 25–30.
[37] T.-T. Kuo, L. Ohno-Machado, Modelchain: decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks, preprint, arXiv:1802.01746, 2018.

[38] M. Wang, Y. Guo, C. Zhang, C. Wang, H. Huang, X. Jia, Medshare: a privacy-preserving medical data sharing system by using blockchain, IEEE Trans. Serv. Comput. (2021).
[39] W. Song, B. Wang, Q. Wang, C. Shi, W. Lou, Z. Peng, Publicly verifiable computation of polynomials over outsourced data with multiple sources, IEEE Trans. Inf. Forensics Secur. 12 (10) (2017) 2334–2347.