Journal of Mechanics in Medicine and Biology
Vol. 25, No. 5 (2025) 2540040 (18 pages)

DOI: 10.1142/S0219519425400408

World Scientific
www.worldscientific.com

ENHANCING HEALTHCARE DATA-SHARING SECURITY WITH BLOCKCHAIN AND POST-QUANTUM CRYPTOGRAPHY

JEN-WEI HU

Network and Security Division
National Center for High-Performance Computing (NCHC), Tainan, Taiwan
hujw@narlabs.org.tw

Received 5 August 2024
Accepted 25 November 2024
Published 6 May 2025

With the rapid advancement of healthcare technologies, Electronic Medical Records (EMRs), have become invaluable resources for enhancing public health. However, these data are typically managed by the healthcare service systems of individual medical institutions. Due to privacy concerns and the complexity of system integration, many institutions are hesitant to share their data, leading to the formation of data silos. The emergence of blockchain technology offers a promising solution for facilitating cross-institutional health data sharing within the Internet of Medical Things (IoMT). Nevertheless, blockchain technology, while promising, has limitations in fully safeguarding privacy. In this paper, we propose a secure and efficient user-centric data-sharing system based on consortium blockchain technology. To ensure robust privacy protection in cross-institutional transactions, our scheme employs lattice-based cryptography, a quantum-resistant cryptographic technique. Additionally, we propose an enhanced proxy re-encryption mechanism that enables granular access control over outsourced data and mitigates the risk of collusion between semi-trusted cloud servers and unauthorized data requesters. Furthermore, our system grants data owners complete control over their medical data, empowering them to selectively share information while maintaining the privacy of sensitive details across different institutions. Through rigorous security and experimental analyses, our scheme is shown to be more efficient and practical than existing alternatives. Moreover, when evaluating performances across various medical data sizes, our scheme significantly reduces computational overhead compared to other systems.

Keywords: Electronic medical records; blockchain; lattice cryptography; proxy re-encryption; healthcare data sharing.

1. Introduction

In recent years, advancements in Artificial Intelligence, Cloud Computing, and Big Data Analytics, along with the global impact of the COVID-19 pandemic, have significantly transformed traditional models of health data collection, storage, and management.[1–4] These innovations have driven the digital transformation and modernization of traditional medical services. Central to this transformation is the

increasing reliance on healthcare data, particularly Electronic Medical Records (EMRs), which contain critical information such as a patient's medical history, diagnoses, treatment procedures, and prescribed medications. EMRs have become indispensable in the healthcare industry, with their market value soaring from nearly nonexistent in 2000 to over $31 billion annually by 2018, driven by the proliferation of the internet and information technology.[5] However, EMRs are often fragmented across various independent healthcare systems managed by different medical institutions, leading to the formation of data silos.[6,7] Privacy concerns and the complexity of system integration further impede the sharing of EMRs between institutions. Consequently, isolated data offer limited potential for comprehensive analysis, the development of more effective treatment techniques, and drug discovery.[8] Therefore, developing a secure cross-institutional health data-sharing scheme is an urgent research priority, necessary for both privacy protection and maximizing the value of health data.

To address the limitations of data sharing in the current healthcare system, blockchain technology offers a promising solution for securely and efficiently managing and sharing EMRs across various healthcare service systems. Public blockchains, such as MedRec,[9] Fortified-Chain,[10] MEdge-Chain,[11] and BCHealth,[12] have been deployed to create fully decentralized platforms for both individuals and institutions. In contrast, consortium blockchains, including Healthchain[13] and MedShare,[14] support multicenter platforms for loosely connected networks of medical institutions. While public blockchains are highly resistant to data tampering, consortium blockchains provide several advantages, including lower costs, higher Transactions Per Second (TPS), and the ability to maintain data privacy without exposing information publicly.[3] Consequently, consortium blockchains are more commonly adopted in practice, particularly within the healthcare industry, where privacy and efficiency are critical concerns. Despite these advancements, challenges persist in safeguarding the privacy protection and security of sensitive health data.

Given the sensitive nature of patient medical records, privacy protection is paramount in health data sharing. Cryptographic technology serves as a cornerstone in safeguarding this protection. Various cryptographic techniques have been proposed to fulfill specific functions: encryption and decryption algorithms ensure data confidentiality[15,16]; signature schemes verify identities and authenticate information;[17,18] and searchable encryption algorithms enable secure and accurate data retrieval.[19,20] The medical cloud service provider, often considered a semi-trusted third party responsible for managing patient information, poses a potential risk of tampering with, abusing, or disclosing EMR information. In cross-institution health data-sharing, it is imperative to maintain data owners' control over access. Proxy Re-Encryption (PRE) is an effective solution by enabling data owners to grant access to their encrypted data without compromising data confidentiality.[2] This approach ensures that only authorized individuals can access the data while preserving the privacy of health records throughout the sharing process. Moreover, data owners

retain control over their data and can leverage zero-knowledge proofs, such as Verifiable Credentials (VCs), to meet conditions on user data without revealing the actual data.[21,22] Furthermore, with the rapid advancements in quantum computing, quantum-resistant algorithms must be considered. Lattice cryptography, which relies on NP-hard mathematical problems, is a promising method to resist quantum attacks.[23,24] These algorithms use cryptographic primitives like lattice structures instead of factorization to create public key schemes that can avoid potential threats posed by Shor's algorithm.[25]

Therefore, to meet the security and privacy-preserving requirements in health data-sharing scenarios, we propose a user-centric data-sharing scheme leveraging blockchain technology. The key contributions of this work are as follows:

(1) A lattice-based data-sharing scheme is proposed to enhance quantum-resistant privacy security for cross-institutional transactions. This scheme employs a modified proxy re-encryption mechanism to prevent unauthorized access, thereby safeguarding the privacy and security of medical data.
(2) Data owners maintain complete control over their data, with a temporary Verifiable Credential (VC) issued to represent their consent for each requester. The user-centric mechanism empowers data owners to issue distinct VCs for different requesters, specifying varying levels of access while safeguarding the privacy of information they choose not to disclose.
(3) The proposed scheme is shown to meet all specified security requirements, including decentralization, data confidentiality, anti-collusion, and quantum resistance, through rigorous theoretical security analysis. In terms of performance simulation, our scheme demonstrates a reduction in computational overhead during the EMR sharing stage, en-compassing encryption, re-encryption, and de-cryption. While the performance during the re-encryption key generation stage is slightly lower, particularly as the number of shares increases, the overall computational overhead of our scheme remains significantly lower than existing related schemes.

The rest of this paper is organized as follows: Section 2 introduces related works. In Sec. 3, we describe the relevant preliminaries used in our scheme. Section 4 presents the proposed scheme in detail. Section 5 provides the security and performance analysis, followed by the conclusions and future work in Sec. 7.

2. Related Works

Blockchain technology can ensure data integrity and security, facilitating the interoperability of health data across different healthcare institutions. Researchers have made significant efforts to develop solutions that leverage this technology for secure and efficient data sharing. Cao *et al.*[3] proposed a blockchain-based electronic health system designed to resist impersonation attacks while ensuring that patients'

EMRs are neither tampered with nor forged. MedRec[9] is another blockchain-based medical records management system that utilizes smart contracts to manage access control and record sharing. Healthchain[13] introduces a health data-sharing platform that uses a pricing game model to optimize both price and system benefits. In Ref. 26 a blockchain-based data-sharing scheme was described, which traces maliciously modified data by storing the original data and transaction data on separate blockchains. However, as the amount of data on the blockchain increases, this approach also increases the storage burden on the chain.

To overcome this challenge, Liu *et al.*[4] proposed a fine-grained controllable file access scheme that combines blockchain with cloud services to prevent privacy leakage. Xia *et al.*[1] presented a blockchain-based data-sharing solution aimed at resolving access control issues associated with storing sensitive data on untrusted cloud servers. Mani *et al.*[27] developed an EMR management system that utilizes the InterPlanetary File System (IPFS) as a storage medium, with the hash of IPFS-stored data recorded on the blockchain, effectively mitigating blockchain storage issues. Bao *et al.*[18] designed a group signature protocol for health data sharing that integrates blockchain with IPFS[28,29] for distributed medical data exchange. However, these approaches may lack sufficient security measures when medical data are stored in cloud or IPFS environments, raising concerns about potential data leakage.

To secure sensitive EMR data on semi-trusted cloud servers, Thwin *et al.*[30] introduced a fine-grained access control model using proxy re-encryption, which safeguards EMRs and allows for revocation. However, this scheme relies on a semi-trusted cloud server that has access to user identities during the registration phase, posing a security risk due to centralized identity management. Liu *et al.*[2] proposed a remote healthcare data-sharing scheme based on an on-chain/off-chain model to address the storage burden associated with medical blockchain data. They also enhanced the proxy re-encryption mechanism to prevent collusion between semi-trusted cloud servers and unauthorized data requesters. Lin *et al.*[31] established a blockchain scheme integrated with the IoMT framework to preserve privacy, enabling mutual user authentication through a message authentication protocol and key generation mechanism. Li *et al.*[32] designed a Designated Verifier Aggregate Signature (DVS) scheme to protect health data privacy within a permission IoMT system. However, these schemes still rely on traditional cryptographic q-order multiplicative cyclic groups, making them vulnerable to attacks from quantum computers. Cai *et al.*[33] proposed a lattice-based DVS protocol that offers enhanced security against quantum attacks for health data sharing in IoMT systems. Li *et al.*[8] introduced an MCF model with a DVS scheme that supports cross-chain health data sharing and ensures data integrity, preventing tampering. This scheme also integrates lattice cryptography, providing resistance against quantum attacks.

Therefore, to enhance the privacy and security of medical data in blockchain-based IoMT systems, this paper proposes the design of a user-centric and more secure data-sharing scheme that utilizes lattice cryptography to improve resistance against quantum attacks.

3. Model and Scheme Overview

A. System Model

Given the highly sensitive nature of the information contained in EMRs and the critical need to protect patient privacy and securing personal medical data in healthcare data- sharing scenarios. To address this need, we propose a medical data-sharing scheme based on lattice cryptography to protect participants' identity privacy. Our proposed system model, shown in Fig. 1, comprises the following entities: User Node (UN), Hospital Node (HN), Management Node (MN), and Cloud Server (CS). In this system, UN, HN, and MN establish a Consortium Blockchain (BC) Network that synchronizes specific data to the blockchain.

- User Node (UN): In our model, UNs include both data owners and data requesters. Data owners, such as patients, retain control over their EMRs and can choose to share them with researchers within the system. Data requesters, typically medical insurance companies or researchers, seek permission from data owners to access these EMRs.
- Hospital Node (HN): HN represents major hospitals and medical research centers. Its primary role is to generate participant medical data (e.g., EMRs) and create EMR abstracts. To ensure data integrity, HN signs these EMRs and abstracts with its public key. Unlike in traditional settings, HN transfers EMR ownership to participants, who then store the data in their digital wallets.
- Management Node (MN): MN serves as the supervisory entity for medical institutions, primarily responsible for regulatory compliance auditing. MN also handles issuing and managing UN identities and generating blocks in the consortium blockchain network. The MNs are divided into two roles: Leader (MN_L) and Follower (MN_F). A leader is dynamically elected among MNs, with followers replicating its decisions.
- Consortium Blockchain (BC): The BC stores metadata, access logs, and verifiable credentials for the scheme. Access to the BC is restricted to a selected group of

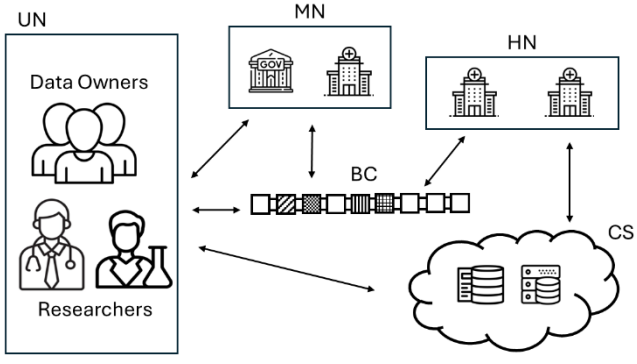


Fig. 1. System model.

authorized consortium members, ensuring secure and efficient collaboration among participants.
- Cloud Server (CS): CS is a third-party cloud provider, either a public cloud or a private cloud maintained by government entities. It is responsible for storing participants' encrypted EMRs and abstracts.

B. Security Requirements

The detailed security requirements for healthcare data sharing are presented as follows:

- The Sybil attack occurs when an adversary creates multiple fake identities to gain excessive influence and control within a healthcare system.
- In the proposed scheme, a semi-trusted entity (CS) is responsible for storing EMRs. However, there is a potential risk that its curiosity may lead to unauthorized access to this healthcare data.
- A replay attack occurs when an adversary intercepts, delays, and retransmits a valid data transmission.
- A collusion attack occurs when adversaries cooperate to gain unauthorized influence in a system. For instance, CS may conspire with data requesters to obtain unauthorized access to EMRs.

C. Preliminaries

(1) **Lattice**

We use $\mathbb{R}$ and $\mathbb{Z}$ to denote the sets of real numbers and integers, respectively. Let M represent the message set, whose elements are polynomials with coefficients belonging to $\{0 \text{ and } 1\}$. The notation $||b||$ and $||B||$ represent the Euclidean norms of column vector (polynomial) b and matrix B, respectively. The notation $||\tilde{B}||$ denotes the Euclidian norm of the Gram-Schmidt orthogonalization of matrix B. We define $||v||_\infty$ as the infinite norm of the column vector (polynomial) v.

Let $b_1, \cdots, b_n \in \mathbb{R}^m$ be vectors that are linearly independent in the Euclidean space. The lattice $L(B) = L(b_1, \cdots, b_n) = \{\sum_{i=1}^{n} z_i b_i | z_i \in \mathbb{Z}, b_i \in \mathbb{R}^m\}$. Generally, when $n = m$, the lattice is referred to as a full-rank lattice. We employ special lattices in algorithms TrapGen and SamplePre,[25] their definitions are given as follows:

$$\wedge_q^{\perp}(B) = \{z \in \mathbb{Z}^m | Bz = 0 \bmod q, B \in \mathbb{Z}_q^{n \times m}\}$$

$$\wedge_q^{u}(B) = \{z \in \mathbb{Z}^m | Bz = u \bmod q, B \in \mathbb{Z}_q^{n \times m}, u \in \mathbb{Z}_q^{n}\}$$

(2) **RLWE**

The RLWE distribution[34] is defined as follows: Let $\mathcal{R} = \mathbb{Z}[x]/(x^n + 1)$, where n is a power of 2. The ring $\mathcal{R}_q = \mathcal{R}/q = \mathbb{Z}_q[x]/(x^n + 1)$, where q is a prime number satisfying $q = 1 \bmod 2n$. Let ψ_a be an error distribution closely related to the discrete Gaussian distribution over $\mathcal{R}_q$. The secret s is uniformly sampled from $\mathcal{R}_q$, and the

error term e is independently sampled according to ψ_a. The distribution A_{s,ψ_a} of (a and b) over $\mathcal{R}_q \times \mathcal{R}_q$ is defined by the equation $= as + e$.

(3) **Proxy Re-encryption**

In this concept, a semi-trusted proxy can acquire a re-encryption key from the data owner. The proxy can then convert the encrypted message under the data owner's public key into an encrypted message under the data requester's public key, without knowing the message.[2,21] The formal definition of the unidirectional identity-based proxy re-encryption is as follows:

- $\text{Setup}(k) \rightarrow \text{pp}$: For this algorithm, input a secret parameter k and output the public parameter pp and the master secret key msk.
- $\text{Extract}(\text{pp},\ \text{id},\ \text{msk}) \rightarrow \text{sk}_{\text{id}}$: Input the public parameters pp, the user's identity id, and the master secret key msk. The algorithm outputs the private key sk_{id} for the user id.
- $\text{Enc}(\text{pp}, \text{id}, M) \rightarrow C_{\text{id}}$: Given pp, id, and a message M as input parameters, this algorithm produces the ciphertext C_A as output.
- $\text{ReKeyGen}(\text{sk}_{\text{id}}, \text{sk}_{\text{id}'}) \rightarrow \text{rk}_{\text{id}\rightarrow\text{id}'}$: Input the private keys sk_{id} and $\text{sk}_{\text{id}'}$. The algorithm generates a re-encryption key $\text{rk}_{\text{id}\rightarrow\text{id}'}$.
- $\text{ReEnc}(C_{\text{id}}, rk_{\text{id}\rightarrow\text{id}'}) \rightarrow C_{\text{id}'}$: The re-encryption algorithm takes the ciphertext C_{id} and the re-encryption key $\text{rk}_{\text{id}\rightarrow\text{id}'}$ as inputs to generate the re-encrypted ciphertext $C_{\text{id}'}$.
- $\text{Dec}(C_{\text{id}'}\text{sk}_{\text{id}'}) \rightarrow M$: Inputs $\text{sk}_{\text{id}'}$ and ciphertext $C_{id'}$yield the message M with overwhelming probability.

4. The Proposed Scheme

A. Overview of the Scheme

The proposed scheme designs a healthcare data-sharing mechanism that includes five main phases. The definitions for each of the symbols used in this study are shown in Table 1. As is illustrated in Fig. 2, the detailed system operation process is as follows:

1. The user generates a private key f_{PID_A} and a public key pk_{PID_A} based on $\text{Setup}(k)$, and registers the public key pk_{PID_A} on the blockchain.
2. The user prepares Info_A and pk_{PID_A} for verification by the Management Node (MN).
3. Upon successful verification, the MN generates the pseudo identity PID_A.
4. After a diagnosis in the Hospital Node (HN), EMR_A and the corresponding metadata M are generated.
5. The metadata are stored on the blockchain by invoking a smart contract, while EMR_A is encrypted using Enc() and stored in the Cloud Server (CS).

Table 1. Symbol description.

Symbol	Description
q	Prime, reducing the coefficient of the polynomial during encryption and decryption
$\mathcal{R}$	Polynomial ring $\mathbb{Z}[x]/(x^n+1)$
$\mathcal{R}_q$	Polynomial ring $\mathbb{Z}_q[x]/(x^n+1)$
n	The dimension of polynomial in rings $\mathcal{R}$ and $\mathcal{R}_q$
mid_i	The identity of the managerment node MN_i
hid_i	The identity of the hospital node HN_i
H_1, H_2	Hash functions
$f_{\mathrm{id}_N}, \mathrm{sk}_{\mathrm{id}_N}$	The private key of id_N
$\mathrm{pk}_{\mathrm{id}_N}$	The public key of id_N
$f_{\mathrm{id}_N}^{-1}$	Multiplicative inverse of polynomail f_{id_N}

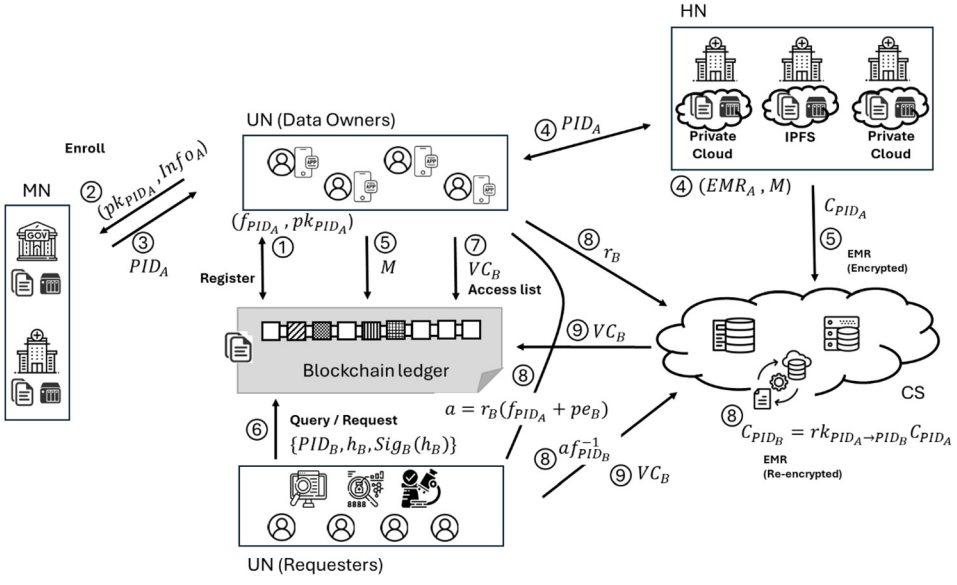


Fig. 2. System operation process.

6. Researchers or doctors can query and request specific medical data by sending PID_B to obtain permission from the data owner.
7. Once the data owner accepts the request, a temporary Verifiable Credential (VC) is issued to represent the data owner's consent for the requester. This VC will allow selected disclosure, where the data owner independently decides what information to share. In addition to the VC, a re-encryption key will be generated via ReKeyGen() and provided to the requester.
8. The CS will receive r_B generated by the data owner and $\mathrm{af}_{\mathrm{PID}_B}^{-1}$ provided by the requester. Using these two pieces of information, the CS can execute ReKeyGen() to generate a re-encryption key and use it to perform ReEnc() producing C_{PID_B}.

9. When requesters query medical data access, they provide the verifiable credential obtained from the data owner to the Cloud Server (CS). The smart contract on the Blockchain (BC) verifies the scope of access permitted for the requesters and grants the corresponding services.

B. Protocol Description

(1) **Initialization**

Given a security parameter $k \in \mathbb{Z}$, a prime number $q = poly(k)$, a prime number $p = 2$, and an integer n. Here, $q = 1 \mod 2n$ and n is a power of 2. The hash functions $H_1 : \{0,1\}^* \to \{-1,0,1\}^n$and $H_2 : \{0,1\}^* \times \{0,1\}^* \to \{-1,0,1\}^n$ are defined. A random matrix $B \in \mathbb{Z}_q^{k \times n}$ and a short trapdoor basis $T_B \in \wedge_q^{\perp}(B)$ are generated by the function $TrapGen(k,q,n)$. The distribution of B is statistically close to uniform distribution over $\mathbb{Z}_q^{k \times n}$ and the length $||\tilde{T_B}|| \leq O(\sqrt{k \log q})$. T_B serves as the master private key of MN.

The set of hospital node is $\mathrm{HN}_1, \mathrm{HN}_2, \cdots, \mathrm{HN}_N$, and each assigned an identity $\{\mathrm{hid}_1, \mathrm{hid}_2, \cdots, \mathrm{hid}_N\}$ Similarly, $\{\mathrm{mid}_1, \mathrm{mid}_2, \cdots, \mathrm{mid}_N\}$ represent the identities of the management nodes. Each node of MNs and HNs obtains its private key according to the following process:

- Suppose a node is N and id_N denoted its identity. It uses the function SamplePre $(B, T_B, H_1(\mathrm{id}_N), \sigma)$ to generate a vector f'_{id_N} whose distribution is statistically close to $D_{\wedge_q^{H(\mathrm{id}_N)}(B),\sigma}$.
- Node N randomly chooses u_{id_N}, which is uniformly sampled with coefficients belonging to $\{-1,0,1\}$ over to $\mathcal{R}_q$ and samples f_{id_N} and g_{id_N} to satisfy the following equations:

$$f_{\mathrm{id}_N} = \{(pf'_{\mathrm{id}_N} + 1) | f_{\mathrm{id}_N} \bmod q \in \mathcal{R}_q^{\times}\}$$

$$g_{\mathrm{id}_N} = \{(g_{\mathrm{id}_N} \in D_{\mathbb{Z}^n,\sigma}) | g_{\mathrm{id}_N} \bmod q \in \mathcal{R}_q^{\times}\}$$

- Here, f_{id_N} is the private key of N, denoted as $\mathrm{sk}_{\mathrm{id}_N}$, while its public key is $\mathrm{pk}_{\mathrm{id}_N} = g_{\mathrm{id}_N} f_{\mathrm{id}_N}^{-1} + u_{\mathrm{id}_N}$.

Upon completion of this initialization phase, the public system parameters are $\{k, q, p, n, B, H_1, H_2, \langle pk_{\mathrm{hid}_i} \rangle_{i=1 \sim N}, \langle pk_{\mathrm{mid}_i} \rangle_{i=1 \sim N}\}$.

(2) **Registration**

We suppose Alice wants to register as a UN. First, using the method mentioned in the initialization phase, Alice can obtain her private key f_{PID_A} and public key $\mathrm{pk}_{\mathrm{PID}_A} = g_{\mathrm{PID}_A} f_{\mathrm{PID}_A}^{-1} + u_{\mathrm{PID}_A}$. Then, she organizes her real identity information Info_A = {Name, Id, Email, Phone} Here, Id refers to the identity card ID or the health insurance card ID given by the MN. Alice stores Info_A in her digital wallet and presents it along with her identity card to the MN for verification. Upon completing

the verification, the MN generates the pseudo identity PID_A for Alice, which she keeps in her digital wallet.

(3) **Encryption and Storage of EMRs**

During each clinic visit to the HN for diagnosis, Alice receives EMR_A along with its summary information, referred to as Info_s. Both are generated by professional physicians at the HN and are signed by the HN to ensure data accuracy. Alice stores the EMR_A in the CS for future data-sharing purposes, while the summary information is temporarily kept for use in the subsequent steps of the process. To securely protect her medical record EMR_A, Alice uses the following steps to encrypt EMR_A before uploading it to the CS:

- Randomly select two noises $b, \nu \in \psi_a$ over $\mathcal{R}_q$.
- Compute ciphertext

$$C_{\mathrm{PID_A}} = p(pk_{\mathrm{PID_A}} b + v) + \mathrm{EMR}_A$$

Alice sends the message $C_{\mathrm{PID_A}}, \delta_A, \sigma_A$ to CS, where δ_A is the hash value of $H_2(C_{\mathrm{PID_A}}, \mathrm{PID}_A)$ and σ_A is the signature of Alice.

After receiving $\{C_{\mathrm{PID_A}}, \delta_A, \sigma_A\}$ from Alice, the CS computes $\delta_A^* = H_2(C_{\mathrm{PID_A}}, \mathrm{PID}_A)$ and verifies whether $\delta_A^* = \delta_A$. The CS also confirms that the signature σ_A belongs to Alice. Once the verification is successful, the CS stores $\{C_{\mathrm{PID_A}}, \delta_A, \sigma_A\}$ and generates a download link (named *url*) for EMR_A.

(4) **Store Metadata on Blockchain**

Upon receiving the download link url, Alice generates the metadata $M = \{\mathrm{url}, \mathrm{Info}_s, \mathrm{PID}_A\}$ and broadcasts the on-chain request $\mathrm{Tx_{req}} = \{M, r_{\mathrm{MN}_L}, h_M, \mathrm{Sig}_A(h_M)\}$ to the consortium blockchain network. Here, r_{MN_L}, generated by the leader of the MN, is a unique and random value used only once in a transaction. h_M represents the hash value of M, and $\mathrm{Sig}_A(h_M)$ denotes Alice's signature on h_M. In our scheme, HNs are responsible for verifying the request by checking the integrity of M and $\mathrm{Sig}_A(h_M)$. Subsequently, each HN generates the endorsement message and sends it to MN_L, where the content is denoted as $E = \{\mathrm{Tx_{req}}, \mathrm{res}, h_E, \mathrm{Sig_{HN}}(h_E)\}$. Here, $\mathrm{Tx_{req}}$ refers to the original request, res indicates the verification result, h_E represents the hash value of $(\mathrm{Tx_{req}}|\mathrm{res})$, and $\mathrm{Sig_{HN}}(h_E)$ is the signature of the current HN. MN_L first checks the integrity of all received E. Then, it retrieves the field res and accumulates the count of all res values set to "agree". If this count exceeds the predefined threshold, MN_L places $\mathrm{Tx} = E$. $\mathrm{Tx_{req}}$ into the transaction pool.

The number of transactions in a block depends on the configuration parameters related to the desired size and maximum elapsed duration for a block. If either of these parameters is satisfied, MN_L constructs a block $\mathrm{Block} = \{\mathrm{Tx}_1, \mathrm{Tx}_2, \cdots, \mathrm{Tx}_n,$ where Tx_k is the confirmed transaction. Then, MN_L generates a block message $\mathrm{BM} = \{\mathrm{Block}, \mathrm{num}, h_B, \mathrm{Sig_{MN}}(h_B)\}$ and distributes it to the consortium blockchain

network (BC). In our proposed system, the blocks generated by MN_L are considered final. Once a transaction is recorded in a block, its position in the ledger is immutable.

Each HN validates the integrity of BM and the validity of the signature. If the verification process passes, the ledger is updated consistently across all nodes. Once ledgers of all nodes have been consistently updated, MN_L selects the next leader mid_j using the formula $j = (R \bmod N) + 1$ where R is a random number generated by MN_L.

(5) **Authorization and Access**

Suppose that researcher Bob finds Alice's metadata relevant to his research. He sends a request message to Alice, asking for her permission to access her EMR_A. The message is $\{\mathrm{PID}_B, h_B, \mathrm{Sig}_B(h_B)\}$, where h_B represents the hash value of PID_B, and $\mathrm{Sig}_B(h_B)$ denotes Bob's signature on h_B.

When Alice receives the request and allows Bob to access her EMR_A, she randomly selects $r_B \in \mathcal{R}_q$ and e_B from the distribution ψ_a over $\mathcal{R}_q$, and then computes $a = r_B(f_{\mathrm{PID}_A} + \mathrm{pe}_B)$. Through secure channels, Alice encrypts a with Bob's public key and transmits it to Bob, while she sends the encrypted r_B with CS's public key to the CS. Bob retrieves a using his private key, then calculates $b = af^{-1}_{\mathrm{PID}_B}$ and sends b to the CS. When the CS receives r_B and b, it calculates the re-encryption key $rk_{\mathrm{PID}_A \to \mathrm{PID}_B} = (f_{\mathrm{PID}_A} + \mathrm{pe}_B) f^{-1}_{\mathrm{PID}_B}$. Then, the CS computes a new ciphertext

$$C_{\mathrm{PID}_B} = \mathrm{rk}_{\mathrm{PID}_A \to \mathrm{PID}_B} C_{\mathrm{PID}_A}$$

Bob downloads the information $\{C_{\mathrm{PID}_B}\}, \delta_A$ from the corresponding url. Then, he validates the integrity of EMR_A by checking whether δ_A equals $H_2(C_{\mathrm{PID}_A}, \mathrm{PID}_A)$. If the verification process passes, Bob decrypts C_{PID_B} to retrieve EMR_A by calculating $(f_{\mathrm{PID}_B} C_{\mathrm{PID}_B}) \bmod q$.

5. Security Analysis

A. Data Confidentiality

Due to the persistent nature of blockchain, data cannot be deleted once written, ensuring data integrity and security, which is a vital aspect of blockchain technology. However, as the amount of data increases, this characteristic leads to ongoing storage challenges that blockchain systems must manage. To mitigate these storage issues, our proposed scheme, like other literature,[2] stores the main body of EMRs on semi-trusted cloud servers. When a data owner authorizes a data requester to access her EMRs, the scheme delegates the Cloud Server (CS) to convert a new ciphertext using the re-encryption key generated by the Identity-Based Proxy Re-Encryption (IB-PRE) mechanism. The data requester can retrieve the EMRs from this new ciphertext using their private key. During the process, the CS is solely responsible for storing encrypted EMRs and facilitating the re-encryption process; It cannot access

the data owner's actual information. Therefore, the proposed scheme ensures data confidentiality.

B. Sybil Attack

In our scheme, the identity verification process ensures that each participant registers only once with a verified identity, thereby preventing the creation of multiple accounts. Digital wallets securely store verified information, preventing tampering or duplication of identities. By acting as a secure repository for the data owner's identity information and cryptographic keys, the digital wallet makes it challenging for attackers to compromise or steal identities. This identity verification process provides robust protection against Sybil attacks by ensuring all participants are genuine and uniquely identified. It enhances the trustworthiness and security of the consortium blockchain, enabling each transaction to be traced back to a verified participant and maintaining the integrity and reliability of the network.

C. Collusion Resistance

In our scheme's authorization and access process, when a data owner receives an authorization request from a data requester, the data owner generates and sends a value a to the data requester, along with the random parameter r_B to the Cloud Server (CS). Even if the data requester obtains r_B from the CS and calculates $a/r_B = f_{\mathrm{PID}_A} + pe_B$, he still cannot obtain due to the presence of the noise polynomial e_B. Similarly, even if the CS obtains f_{PID_B} and calculates $rk_{\mathrm{PID}_A \to \mathrm{PID}_B} f_{\mathrm{PID}_B} = f_{\mathrm{PID}_A} + \mathrm{pe}_B$, it still cannot retrieve the data owner's private key f_{PID_A} due to the noise polynomial e_B. Thus, our proposed scheme ensures collusion resistant between the semi-trusted CS and data requesters.

D. Replay Attack

The random value r_{MN_L} generated by the leader of the MN, serves as a nonce — a unique value used only once in a transaction. This ensures that each transaction request, represented by $\mathrm{Tx}_{\mathrm{req}}$, is unique and cannot be replayed. Additionally, blockchain transactions include timestamps that record the exact time when the transaction is created and added to the blockchain. Therefore, combining r_{MN_L} with the timestamp in blockchain transactions provides dual protection against replay attacks, safeguarding transactions across different sessions and ensuring the immutability of recorded transactions in the ledger.

E. Decryption Correction

Lemma 1. *The data owner can decrypt the ciphertext* $C_{\mathrm{PID}_\mathrm{A}}$ *and retrieve the plaintext* EMR_A *using her private key.*

Proof. The ciphertext C_{PID_A} is defined as

$$C_{\mathrm{PID}_A} = p(\mathrm{pk}_{\mathrm{PID}_A} b + v) + \mathrm{EMR}_A$$

This ciphertext is the result of the encryption algorithm $\mathrm{Enc}(\mathrm{pp},\ \mathrm{id}, M)$. We use the decryption algorithm $\mathrm{Dec}(C_{\mathrm{PID}_A}\mathrm{sk}_{\mathrm{PID}_A})$ to compute

$$\begin{aligned} C'_{\mathrm{PID}_A} &= f_{\mathrm{PID}_A} C_{\mathrm{PID}_A} \bmod q \\ &= f_{\mathrm{PID}_A}(p(pk_{\mathrm{PID_A}} b + v) + \mathrm{EMR}_A) \\ &= f_{\mathrm{PID}_A}(p[(g_{\mathrm{PID}_A} f^{-1}_{\mathrm{PID}_A} + u_{\mathrm{PID}_A})b + v] + \mathrm{EMR}_A) \\ &= pg_{\mathrm{PID}_A} b + f_{\mathrm{PID}_A} u_{\mathrm{PID}_A} b + f_{\mathrm{PID}_A} \mathrm{pv} + f_{\mathrm{PID}_A} \mathrm{EMR}_A \end{aligned}$$

Given that $f_{\mathrm{PID}_A} = \mathrm{pf}'_{\mathrm{PID}_A} + 1 = 1 \bmod p$, we can conclude

$$C'_{\mathrm{PID}_A} \bmod p = \mathrm{EMR}_A$$

Thus, the decryption process successfully retrieves the plaintext EMR_A from the ciphertext. □

Lemma 2. *If the data requester receives the ciphertext* $C_{\mathrm{PID_B}}$*, which was encrypted using the re-encryption key* $\mathrm{rk}_{\mathrm{PID}_A \to \mathrm{PID}_B}$*, she can decrypt and retrieve the plaintext* EMR_A *using her private key.*

Proof. The re-encryption key $\mathrm{rk}_{\mathrm{PID}_A \to \mathrm{PID}_B}$ is generated by the algorithm ReKeyGen $(\mathrm{sk}_{\mathrm{PID}_A}, \mathrm{sk}_{\mathrm{PID}_B})$ and the ciphertext $C_{\mathrm{PID}_B} = rk_{\mathrm{PID}_A \to \mathrm{PID}_B} C_{\mathrm{PID}_A}$ is computed by encryption algorithm $\mathrm{ReEnc}(C_{\mathrm{id}}, rk_{\mathrm{PID}_A \to \mathrm{PID}_B})$. Using the decryption algorithm $\mathrm{Dec}(C_{\mathrm{PID}_B}\mathrm{sk}_{\mathrm{PID}_B})$, we can compute

$$\begin{aligned} C'_{\mathrm{PID}_B} &= f_{\mathrm{PID}_B} C_{\mathrm{PID}_B} \bmod q \\ &= f_{\mathrm{PID}_B}(f_{\mathrm{PID}_A} + \mathrm{pe}_B) f^{-1}_{\mathrm{PID}_B}(p(\mathrm{pk}_{\mathrm{PID}_A} b + v) + \mathrm{EMR}_B) \\ &= (f_{\mathrm{PID}_A} + \mathrm{pe}_B)(p(g_{\mathrm{PID}_A} f^{-1}_{\mathrm{PID}_A} + u_{\mathrm{PID}_A})b + v] + \mathrm{EMR}_B) \\ &= \mathrm{pg}_{\mathrm{PID}_A} b + \mathrm{pf}_{\mathrm{PID}_A} u_{\mathrm{PID}_A} b + \mathrm{pf}_{\mathrm{PID}_A} v + f_{\mathrm{PID}_A} \mathrm{EMR}_B \\ &\quad + p^2 g_{\mathrm{PID}_A} f^{-1}_{\mathrm{PID}_A} e_B b + p^2 e_B u_{\mathrm{PID}_A} b + p^2 e_B v + \mathrm{pe}_B \mathrm{EMR}_B \end{aligned}$$

Finally, since $f_{\mathrm{PID}_A} = pf'_{\mathrm{PID}_A} + 1 = 1 \bmod p$ and the sum of the other terms (except $f_{\mathrm{PID}_A}\mathrm{EMR}_B$) is zero modulo p, we have that $C'_{\mathrm{PID}_B} = \mathrm{EMR}_B \bmod p$. □

6. Performance Analysis

A. Functional Features

In this section, our proposed scheme is compared with similar schemes in terms of security features, including decentralization, confidentiality, integrity, quantum resistance, anti-collusion security, and user-centric access control. Table 2 demonstrates that our scheme fulfills all functional requirements. Notably, while [8] our scheme can resist post-quantum attacks, it[8] lacks mechanisms for user-defined access control and anti-collusion security. While[2] our scheme offers anti-collusion security, other schemes do not meet this criterion. However,[2] it relies on a q-order multiplicative cyclic group, which limits its ability to resist quantum cryptography attacks.

Table 2. Comparison of function features.

Functionality	Liu *et al.*[2]	Li *et al.*[32]	Li *et al.*[8]	Ours
Decentralization	✓	✓	✓	✓
Confidentiality	✓	✓	✓	✓
Data integrity	✓	✓	✓	✓
Anti-collusion	✓	×	×	✓
Quantum-resistant	×	×	✓	✓
User-defined access control	×	×	×	✓

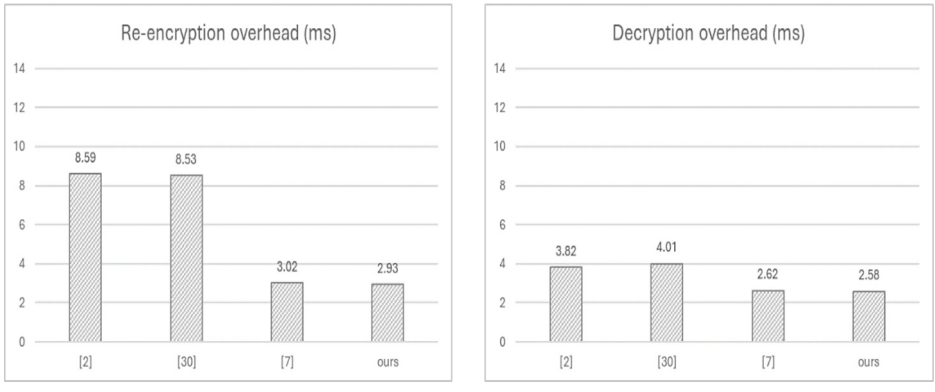
B. Performance Analysis

The performance of the proposed model is evaluated by comparing its computational overhead to that of other schemes. Since proxy re-encryption is the core component in all schemes, the experiments are divided into four main stages: encryption, re-encryption key generation, re-encryption, and decryption. For the cryptographic operation comparison, all experiments are conducted on a system with an Intel(R) Core i7-8559U CPU, 2.70 GHz, 8 GB memory running a 64-bit Linux operating system. Each scheme is implemented using the Java Pairing-Based Cryptography[35] and NTRUReEncrypt[36–38] libraries. A Hyperledger blockchain network, created in a Docker environment, is used for blockchain service testing, comprising orderer nodes, endorser nodes, and three peer nodes.

According to Fig. 3(a), the encryption stage of our scheme requires significantly less time than the other schemes. In the re-encryption key generation stage, Fig. 3(b) shows that our scheme's performance is second only to the scheme in Ref. 2. However, as illustrated in Figs. 3(c) and 3(d), our scheme performs best in the re-encryption and decryption stages. Based on this comparison, our model demonstrates better overall performance in the encryption, re-encryption, and decryption stages. Although the re-encryption key generation stage ranks only second, this key

(a) (b)

Fig. 3. Comparison of computational overhead: (a) encryption stage, (b) re-encryption key generation stage, (c) re-encryption stage, (d) decryption stage.

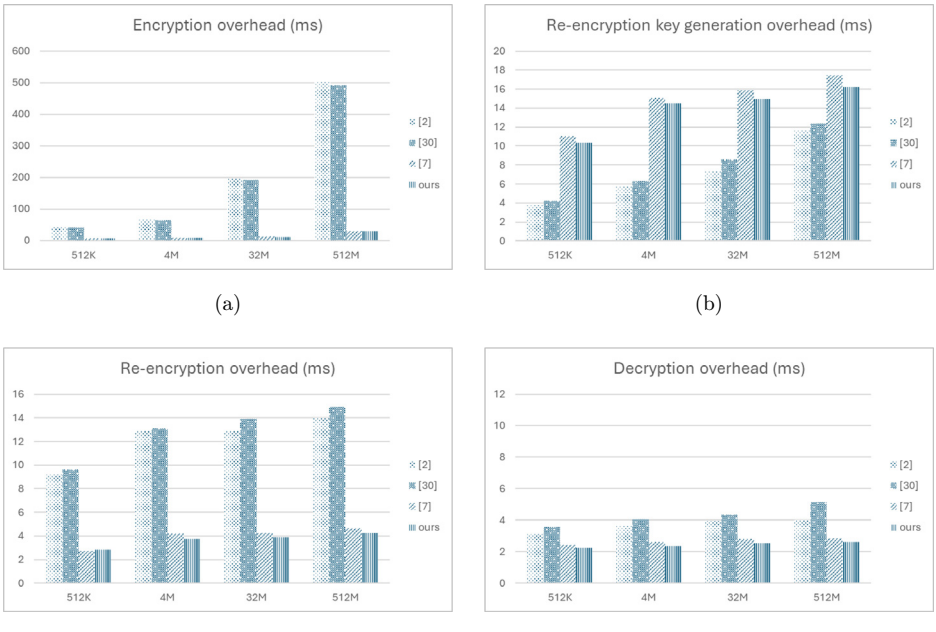


(c) (d)

Fig. 3. (*Continued*)

is typically generated only once when requested by the requester, making its impact on overall performance minimal.

Next, we consider the impact of EMR data size on overall performance by utilizing EMR data of various sizes in our experiment. To construct our experiment,



(a) (b)

(c) (d)

Fig. 4. Comparison of computational overhead based on various EMR data sizes: (a) encryption stage, (b) re-encryption key generation stage, (c) re-encryption stage, (d) decryption stage.

we explored diverse data source. Initially, plaintext EMR records are approximately 169 KB.[9] We also included medical imaging data, which have increased in size due to advancements in imaging technology and higher resolutions. The size of medical imaging data varies significantly depending on imaging modality, resolution, and compression techniques. For instance, the uncompressed sizes of X-ray, CT, and MRI images differ. X-ray images, typically captured at 2048x2048 pixels, range from 10 to 20 megabytes per image. Similarly, a single CT image varies from 0.5 to 10 megabytes, with a full CT scan series typically occupying between 100 to 512 megabytes. MRI images, depending on resolution and slice thickness, range from 0.5 to 5 megabytes per image. To encompass a comprehensive range of data sizes in our experiment, our EMR data include sizes of 512 KB, 4 MB, 32 MB, and 512 MB.

Figure 4 presents the comparisons between different schemes across various EMR data sizes. For each stage, the time required by these five schemes increases with the size of the EMR data. In the re-encryption key generation stage, as shown in Fig. 4(b), our scheme requires more time compared to Ref. 2.However, in the encryption, re-encryption, and decryption stages, depicted in Figs. 4(a), 4(c), and 4(d), respectively, our scheme performs better than the other schemes in terms of computational overhead.

7. Conclusion

Effectively sharing healthcare data across different institutions while protecting personal privacy remains a significant challenge in medical data exchange. In this paper, we propose a secure and user-centric data-sharing scheme based on blockchain technology. The scheme employs lattice-based cryptography, providing resistance against quantum attacks, and leverages a proxy re-encryption mechanism to enhance both privacy and security in system transactions and user interactions. In our scheme, data owners can issue verifiable credentials to various requesters, enabling fine-grained access control. The proposed scheme meets essential security requirements, including data confidentiality, collusion resistance, and protection against Sybil and replay attacks. Both simulation and theoretical analysis demonstrate that our scheme achieves greater efficiency in computational overhead for medical data sharing compared to other approaches. While our scheme ranks second in re-encryption key generation performance, this key is typically generated only once, resulting in minimal impact on overall performance.

Future research directions could focus on improving key generation efficiency, identity authentication, secure secret sharing, and handling revocation in cases of leakage behavior among users. These areas hold promise as fruitful avenues for further exploration.

ORCID

Jen-Wei Hu https://orcid.org/0009-0003-1409-3770

References

1. Xia Q, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M, MeDShare: Trust-less medical data sharing among cloud service providers via blockchain, *IEEE Access* **5**:14757–14767, 2017.
2. Liu J *et al.*, Conditional anonymous remote healthcare data sharing over blockchain, *IEEE J Biome Health Infor* **27**(5):2231–2242, 2023.
3. Cao S, Zhang G, Liu P, Zhang X, Neri F, Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain, *Inf Sci* **485**:427–440, 2019.
4. Liu Y, Zhang J and Gao Q, A blockchain-based secure cloud files sharing scheme with fine-grained access control, in *Proc Int Conf Netw Appl*, IEEE, pp. 277–283, 2018.
5. Nguyen KH *et al.*, Economic evaluation and analyses of hospital-based electronic medical records (EMRs): A scoping review of international literature, *Digit Med* **5**:29, 2022.
6. Sun J and Fang Y, Cross-domain data sharing in distributed electronic health record systems, *IEEE Trans Parallel Distrib Syst* **21**(6):754–764, 2010.
7. Mohana M, Deotare VV, Preetha NSN, Brammy G, An adaptive elliptical curve cryptography-Rivest-Shamir-Adleman-based encryption for IoT healthcare security model with blockchain technology, *J Mech Med Biol* **24**(4):2350068, 2024.
8. Li C *et al.*, Efficient designated verifier signature for secure cross-chain health data sharing in BIoMT, *IEEE Int Things J* **11**(11):19838–19851, 2024.
9. Azaria A, Ekblaw A, Vieira T and Lippman A, MedRec: Using blockchain for medical data access and permission management, in *Proc 2nd Int Conf Open Big Data*, IEEE, pp. 25–30, 2016.
10. Egala BS, Pradhan AK, Badarla V, Mohanty SP, Fortified chain: A blockchain-based framework for security and privacy-assured Internet of Medical Things with effective access control, *IEEE Int Things J* **8**(14):11717–11731, 2021.
11. Abdellatif AA *et al.*, Medge-chain: Leveraging edge computing and blockchain for efficient medical data exchange, *IEEE Int Things J* **8**(21):15762–15775, 2021.
12. Hossein KM, Esmaeili ME, Dargahi T, Khonsari A, Conti M, BCHealth: A novel blockchain-based privacy-preserving architec ture for IoT healthcare applications, *Comput Commun* **180**:31–47, 2021.
13. Li C *et al.*, Healthchain: Secure EMRs management and trading in distributed healthcare service system, *IEEE Int Things J* **8**(9):7192–7202, 2021.
14. Wang M *et al.*, MedShare: A Privacy-preserving medical data sharing system by using blockchain, *IEEE Trans. Services Comput* **16**(1):438–451, 2023.
15. Xu G *et al.*, A privacy-preserving medical data sharing scheme based on blockchain, *IEEE J Biomed Health Inform* **27**(2):698–709, 2023.
16. Guo H, Li W, Nejad M and Shen CC, A hybrid blockchain-edge architecture for electronic health record management with attribute based cryptographic mechanisms, *IEEE Trans Netw Service Manag* **20**(2):1759–1774, 2023.
17. Guo R, Li K, Li X, Zhang Y, Li X, Compact multiple attribute based signatures with key aggregation and its application, *IEEE Syst J* **16**(2):3025–3035, 2022.
18. Bao Z, He D, Wang H, Luo M, Peng C, A group signature scheme with selective linkability and traceability for blockchain-based data sharing systems in E-Health services, *IEEE Int Things J* **10**(23):21115–21128, 2023.
19. Li H, Yang Y, Dai Y, Yu S, Xiang Y, Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data, *IEEE Trans Cloud Comput* **8**(2):484–494, 2020.
20. Liu J *et al.*, Blockchain aided privacy-preserving medical data sharing scheme for e-healthcare system, *IEEE Internet Things J* **10**(24):21377–21388, 2023.

21. Belchior R. *et al.*, Ssibac: Self-sovereign identity based access control, in *Proc 19th Int Conf Trust Sec Privacy Comput Commun (TrustCom)*, IEEE, pp. 1935–1943, 2020.
22. Pujari C, Muniyal B, Chandrakala, CB and Rajarajan M, A user-centric self-sovereign identity-based authentication framework for decentralized data management in healthcare settings, in *Proc Int Conf Recent Adv Inf Technol Sustain Dev (ICRAIS)*, IEEE, pp. 89–94, 2023.
23. Ye Q, Lang Y, Guo H, Tang Y, Efficient lattice-based traceable ring signature scheme with its application in blockchain, *Inf Sci* **648**, 2023, Art. no. 119536.
24. Yu H, Lv Z, Lattice-based ring signcryption for condsortium blockchain, *J King Saud Univ-Comput Inf Sci* **35**(7):2023, Art. no. 101602.
25. Yang Z, Salman T, Jain R, Pietro RD, Decentralization using quantum blockchain: A theoretical analysis, *IEEE Trans on Quantum Eng* **3**:1–16, 2022.
26. Wang Z, Tian Y, Zhu J, Data sharing and tracing scheme based on blockchain, in *Proc 8th Int Conf Logistics*, IEEE, pp. 1–6, 2018.
27. Mani V, Manickam P, Alotaibi Y, Alghamdi S, Khalaf O, Hyperledger healthchain: Patient-centric IPFS-based storage of health records, *Electronics* **10**(23):3003, 2021.
28. Zhan W, Chen CL, Weng W, Tsaur WJ, Deng YY, Incentive EMR sharing system based on consortium blockchain and IPFS, *Healthcare* **10**:1840, 2022.
29. Li L, Yue Z, Wu G, Electronic medical record sharing system based on hyperledger fabric and interplanetary file system, in *Proc 5th Int Conf Comp Data Anal (ICCDA)*, pp. 149–154, 2021.
30. Thwin TT, Vasupongayya S, Blockchain-based access control model to preserve privacy for personal health record systems, *Secur Commun Netw* **2019**:1–15, 2019.
31. Lin Q, Li X, Cai K, Prakash M, Paulraj D, Secure Internet of Medical Things (IoMT) based on ECMQV-MAC authentication protocol and EKMC-SCP blockchain networking, *Inf Sci* **654**:2024, Art. no. 119783.
32. Li T, Wang H, He D, Yu J, Designated-verifier aggregate signature scheme with sensitive data privacy protection for permissioned blockchain-assisted IIoT, *IEEE Trans. Inf Forensics Secur* **18**:4640–4651, 2023.
33. Cai J *et al.*, An efficient strong designated verifier signature based on R—SIS assumption, *IEEE Access* **7**:3938–3947, 2019.
34. Yang N and Tian Y, Identity-based unidirectional collusion-resistant proxy re-encryption from U-LWE, *Secur Commun Netw* **2023**:1–9, 2023.
35. de Caro A, Iovino V, jPBC: Java pairing based cryptography, in *Proc 16th IEEE Symp Computers and Communications (ISCC)*, IEEE, pp. 850–855, 2011.
36. Nunez D, Agudo I, Lopez J, NTRUReEncrypt: An efficient proxy re-encryption scheme based on NTRU, in *Proc 10th ACM Symp Information Computer and Communications Security (ASIA CCS)*, 2015, pp. 179–189.
37. Lemons N *et al.*, A. Nadiga, K. Meier, and R. Newell, Extending quantum key distribution through proxy re-encryption, *J Opt Commun Netw* **15**(7):457–465, 2023.
38. Tzinos1 I, Limniotis K, Kolokotronis N, Evaluating the performance of post-quantum secure algorithms in the TLS protocol, *J Surveill Secur Saf* **3**:101–127, 2022.