mathematics

MDPI

Article

A Blockchain-Based Secure Sharing Scheme for Electrical Impedance Tomography Data

Ruwen Zhao [1,2,3], Chuanpei Xu [1,*], Zhibin Zhu [2,3] and Wei Mo [1]

[1] School of Electronic Engineering and Automation, Key Laboratory of Automatic Detecting Technology and Instruments, Guilin University of Electronic Technology, Guilin 541004, China; zhaoruwen@guet.edu.cn (R.Z.); wmo@guet.edu.cn (W.M.)
[2] School of Mathematics and Computing Science, Guilin University of Electronic Technology, Guilin 541004, China; zhuzb@guet.edu.cn
[3] Center for Applied Mathematics of Guangxi, Guilin University of Electronic Technology, Guilin 541004, China
* Correspondence: xcp@guet.edu.cn

Abstract: Real-time electrical impedance tomography (EIT) data sharing is becoming increasingly necessary, due to the extensive use of EIT technology in various sectors, including material analysis, biomedicine, and industrial process monitoring. The prevalence of portable EIT equipment and remote imaging technology has led to a predominance of centralized storage, Internet protocol transmission, and certificates from certificate authorities (CA) in telemedicine data. This has resulted in compromised data security, network communication delays, high CA maintenance costs, increased risks of medical data privacy breaches, and low security. Therefore, this paper offers a consortia blockchain-based method for exchanging EIT data that addresses security and integrity concerns during data storage and exchange, while maintaining transparency and traceability. Proprietary re-encryption techniques are employed to guarantee traceability when exchanging anonymous data, enabling precise control over data access. This scheme serves to protect both data and identity privacy, as well as to trace the actual identity of potential malicious users, while also thwarting any coordinated efforts between partially trusted parties and data requesters seeking unauthorized access to confidential information. Additionally, a combination of blockchain and InterPlanetary File System (IPFS) distributed storage technology is utilized to ease the burden of EIT data storage. The feasibility and effectiveness of the proposed solution were validated through a series of experiments, demonstrating its ability to effectively prevent data tampering and misuse, reduce data management costs, and enhance the efficiency and quality of data sharing.

Keywords: electrical impedance tomography; data sharing; blockchain; proxy re-encryption

MSC: 94A60

Citation: Zhao, R.; Xu, C.; Zhu, Z.; Mo, W. A Blockchain-Based Secure Sharing Scheme for Electrical Impedance Tomography Data. *Mathematics* **2024**, *12*, 1120. https://doi.org/10.3390/math12071120

Academic Editors: Andrea Scozzari, Jialing He, Zhi Fang and Chunhai Li

Received: 19 March 2024
Revised: 4 April 2024
Accepted: 7 April 2024
Published: 8 April 2024

1. Introduction

With the rapid advancement of medical detection technology, there is a growing demand for more sophisticated medical detection methods [1]. The evolution of detection methods has progressed from manual subjective assessment to a combination of subjective and objective approaches. The introduction of medical imaging technology has significantly enhanced the objectivity and accuracy of disease diagnosis. Electrical impedance tomography (EIT) technology is crucial for achieving this goal [2]. EIT is a novel non-destructive biomedical detection and imaging technique focusing on the distribution or variation in electrical impedance within living organisms [3]. This technology allows visualizing impedance distribution images of biological tissues, impedance change images across different frequencies, and impedance variation images during physiological activities of biological organs, such as respiration and heartbeats [4]. EIT offers the advantages of simplicity, non-invasiveness, affordability, and the potential for long-term and continuous

patient monitoring [5]. It is important in early disease prevention, diagnosis, treatment, and medical screening [6]. Furthermore, the increasing digitization of the medical industry has led to a notable shift towards using electronic medical records (EMR) [7]. EMRs have gained widespread popularity due to their ability to offer convenient and superior electronic medical services. By sharing EMRs among medical institutions, patients can provide real-time and long-term disease information to support in-depth analysis and personalized patient treatment [8].

Protecting sensitive health information within EMRs is paramount to safeguarding patient privacy [9]. Sharing EMR data is crucial for reducing medical costs and improving service quality. However, the scattered storage of EMRs across various medical institutions poses challenges for data sharing and increases the risk of patient privacy breaches [10]. Many hospitals and institutions still rely on traditional databases to store patient information, hindering inter-institutional data sharing and leading to information silos. Cloud storage solves these issues by providing accessibility, scalability, and by addressing privacy and security concerns [11]. Their centralized nature poses potential risks, such as unauthorized access compromising data privacy and security [12]. As the volume of medical data grows, ensuring medical record's security, scalability, and interoperability has become a critical focus.

1.1. Our Contributions

In order to address the issue of secure storage and sharing of EIT data, this paper presents a secure sharing scheme for EIT data that is both anonymous and conditionally traceable. The scheme is built on the alliance blockchain, utilizing IPFS and blockchain technology. The key contributions of this study are outlined as follows:

- The EIT remote imaging system utilizes an anonymous and traceable authentication protocol. By employing pseudo-identity to safeguard user privacy, it has the capability to expose the identity of malicious nodes under certain circumstances and enhance verification efficiency through batch verification. Furthermore, this protocol enables easy implementation of the key recovery function.
- A decentralized architecture inspired by MedRec was developed to establish a trustworthy platform for sharing and collaborating on EIT data. This system integrates the consortium chain with the IPFS to enable both on-chain and off-chain collaborative storage of EIT data. The chain only stores the IPFS hash of the EIT data, while the complete dataset is transferred to IPFS. This approach helps alleviate storage constraints on the chain and ensures secure storage of EIT data.
- The EIT data sharing system employs proxy re-encryption (PRE) technology to enforce stringent access control measures, thereby enhancing data privacy and security, to mitigate the risks of unauthorized disclosure and exploitation. A verifiable random function (VRF) is employed to generate random numbers for selecting the leader (proxy node), with the design ensuring that the random numbers generated for encryption and data access requests thwart potential collusion between semi-trusted agents and data requesters, thus preventing unauthorized access to secret information.

1.2. Related Work

In the field of medical data secure retrieval, research has primarily focused on functionality, security, and retrieval efficiency. Amiri et al. proposed a method that combines permissioned blockchain and private blockchain to support electronic medical record sharing through keyword retrieval [13]. This approach involves storing encrypted electronic medical records on a cloud server, storing the ciphertext hash value on the private chain, and storing the keyword index on the alliance chain. These measures ensure the secure storage, retrieval, and sharing of electronic medical records. Chen et al. presented a method that combines blockchain technology with searchable encryption technology to enable medical image data sharing [14]. This scheme generates trapdoors by creating keywords related to specific medical imaging data and sending them to the cloud server to search

for the corresponding ciphertext. This enables users to conveniently use the blockchain to verify the authenticity of medical record ciphertext. Furthermore, Ren et al. proposed a framework for sharing electronic medical records between different entities using cloud storage and blockchain [15]. In this framework, the cloud server stores electronic medical record ciphertext, the alliance blockchain saves the electronic medical record index, and keyword searchable encryption ensures the secure retrieval of ciphertext data in the chain. A consortium chain network model, data structure, and consensus mechanism were all designed to ensure the efficient operation of the system [16]. However, it is worth noting that, while these methods leverage the decentralized characteristics of blockchain to address the issues of centralized secure retrieval in traditional cloud storage, most of them do not consider the controllability of user retrieval permissions.

Wang et al. proposed a solution utilizing searchable encryption technology to conceal the access structure, enabling data owners to manage user access rights as per their requirements [17]. Xu et al. proposed a cloud-chain collaborative data secure sharing scheme, employing attribute encryption to encrypt electronic medical records and allowing patients to independently set access policies to achieve precise access control [18,19]. Similarly, Ref. [20] presented a scheme for sharing K-anonymous and keyword-searchable encrypted medical data in an alliance blockchain environment. This scheme incorporates an attribute-based access control smart contract, empowering patients with complete control over their medical records. However, this approach also imposes an additional burden on the users. To address the issue of user inability to control the security of medical data and electronic medical record sharing, Ref. [21] proposed a blockchain-based electronic health system. This system employs a proxy re-encryption mechanism and embeds an attribute-based cryptographic system to ensure high security and fine-grained access control. Du et al. introduced a novel business process and blockchain-based platform for sharing medical information [22]. This innovative approach allows secure storage, sharing, and verification of information among multiple parties in a decentralized network. Additionally, the authors suggested a new consensus algorithm and a comprehensive anonymous sharing model, which enhance the efficiency and security of medical information exchange among users. Liu et al. proposed a conditional anonymous telemedicine data sharing scheme that leverages blockchain technology and cloud servers for secure storage and sharing of medical data [23]. It is important to note that, while the aforementioned research began to focus on empowering patients and giving them control over medical records, there is still a lack of research on how hospitals and patients can jointly control access to electronic medical records.

According to research [24], blockchains can be categorized into three types: public chains, private chains, and consortium chains. A public chain, accessible to everyone, is entirely decentralized, due to its immutable data. On the other hand, a consortium chain restricts participation to authorized members, setting rules for access and participation privileges. In contrast, a private chain is exclusive to private organizations, with limited participating nodes and strict permissions for reading, writing, and accounting [16]. Table 1 provides a comparison of the various blockchain types [25].

Table 1. Comparison of different types of blockchain (consortium chain [26], public chain [27], private chain [28], hybrid chain [29]).

	Decentralization	**Throughput**	**Cost**	**Scalability**
Consortium Chain	medium	medium	medium	Great
Public chain	high	low	high	Poor
Private chain	low	high	low	Great
Hybrid chain	-	-	low	Great

1.3. Organization

The organization of this paper is as follows: Section 2 presents some preliminaries regarding Blockchain. Section 3 describes the EIT data security sharing model and its security requirements in detail. In Section 4, we first describe the framework of our propose scheme, and then present the its details. Section 5 analyzes its correctness and safety. Following that, Section 6 explores a theoretical comparison of the computational complexity of our scheme and offers a performance evaluation. Finally, Section 7 gives some conclusive remarks.

2. Preliminaries

2.1. Consortium Blockchain

A consortium blockchain is a hybrid form of blockchain technology that falls between a fully public blockchain and a fully private blockchain. In this model, a pre-selected group of entities or organizations form a federation to jointly control the nodes. Unlike public blockchains, consortium blockchains are restricted to members of the consortium, which typically consist of stakeholders from various industries like banks, supply chain companies, and government agencies. These members collaborate to manage and maintain the blockchain, leading to increased transaction speed and efficiency, due to the limited number of participants and the trust established among them. Key features of consortium blockchains include

(1) Permission-based node management: Not everyone can participate in the maintenance of the blockchain. Only authorized nodes can perform transaction verification and other related operations.
(2) Higher efficiency and scalability: due to the limited number of participants, the network is able to handle higher transaction volumes, while maintaining fast processing speeds.
(3) Privacy: Although transaction data are open to alliance members, they are not public to the outside world, which provides the possibility for sensitive business operations and data protection.
(4) Co-governance: all alliance members jointly determine the rules, protocols, and standards of the blockchain, making the governance of the entire system more democratic and transparent.

Consortium blockchains are often regarded as well suited for enterprise-level applications, due to their ability to merge the decentralization aspects of public blockchains with the control and security of private blockchains. For instance, in sectors like supply chain management, financial services, healthcare, and cross-border payments, consortium blockchains can offer an effective platform for collaboration and foster trust and data sharing among various organizations.

2.2. InterPlanetary File System

IPFS is a distributed file storage protocol aimed at enhancing the openness, efficiency, and durability of the Internet [30]. Utilizing peer-to-peer technology, every network user functions as both a client and a server, leading to a more decentralized and censorship-resistant file storage system [31]. IPFS operates by breaking files into small chunks and assigning a unique hash value to each chunk. These file blocks are then distributed across multiple nodes worldwide, and when a file needs to be retrieved, IPFS uses these hashes to locate and piece together the file blocks to reconstruct the original file [32]. This method significantly enhances data reliability, as even if some nodes are offline or data are partially lost, the file can still be reconstructed, as long as enough data blocks can be located [33]. Figure 1 presents the general architecture of IPFS.

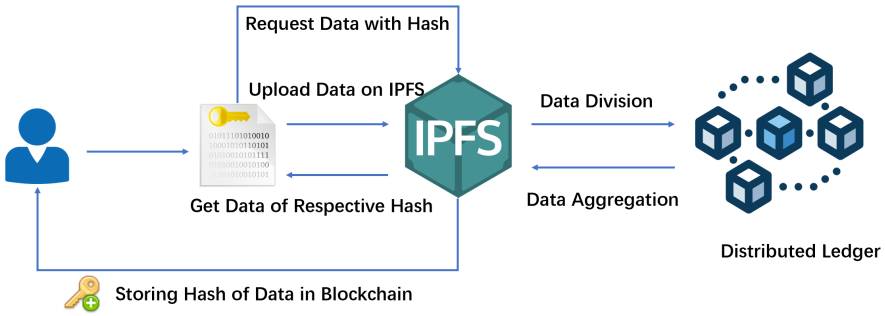

Figure 1. The general architecture of IPFS.

2.3. Proxy Re-Encryption

Proxy re-encryption (PRE) is an encryption method that enables a third party (agent) to convert ciphertext from one secret key to another [34], without the agent having access to the plaintext content. This method is especially valuable in multi-user environments, where securely sharing encrypted data is necessary [35].

The proxy node acts as the leader, holding private key PrK_L and public key PuK_L. Upon receiving $\{r_{i\to j}, sig_r\}$, the proxy node initiates the F. SignVerif algorithm for signature verification. Successful validation grants access to the ciphertext $\{Dec, CEIT_1, CEIT_2, CEIT_3\}$ stored on IPFS, which is then confirmed using Equation (2). Following a positive verification, the proxy node proceeds to re-encrypting the ciphertext, as follows:

$Dec' = E(pk_i, rk_2)$

$CEIT_1{}' = CEIT_1{}^{rk_1}$

$CEIT_2{}' = g_1{}^u$

$CEIT_3{}' = \left(u + PrK_L \mathrm{Hash}_7\left(Dec' \| CEIT_1{}' \| CEIT_2{}'\right)\right) \bmod q$

subsequently creates the re-encrypted text $\{Dec', CEIT_1{}', CEIT_2{}', CEIT_3{}'\}$, and sends it to U_j.

3. System Architecture and Security Requirements

3.1. Blockchain-Based Remote EIT System Architecture

Placing the electrode arrays developed by our team around the patient's chest and applying a small current to them, we can safely measure the voltage difference across the lungs. By adjusting the current injection and measurement points, our system can gather sufficient data to map the entire chest. This method enables the creation of two-dimensional impedance images of the lungs, as different tissues like gas-filled alveoli and water-laden blood exhibit varying resistances to electrical current (comprising resistance and reactance).

In the context of EIT data exchange, individuals use the EIT data sharing system to provide their EMRs to authorized data requesters. However, due to the sensitive nature of EMRs, there are concerns regarding patient privacy, which may result in a reluctance to share personal data. To address this issue and ensure participant anonymity, we propose the implementation of a remote EIT data sharing method. As depicted in Figure 2, the EIT consortium blockchain facilitates the exchange of EIT data between patients and data requesters. The system framework consists of three main components: the EIT data collection module, the EIT consortium blockchain (EITCB), and the IPFS cloud server (IPFSCS).

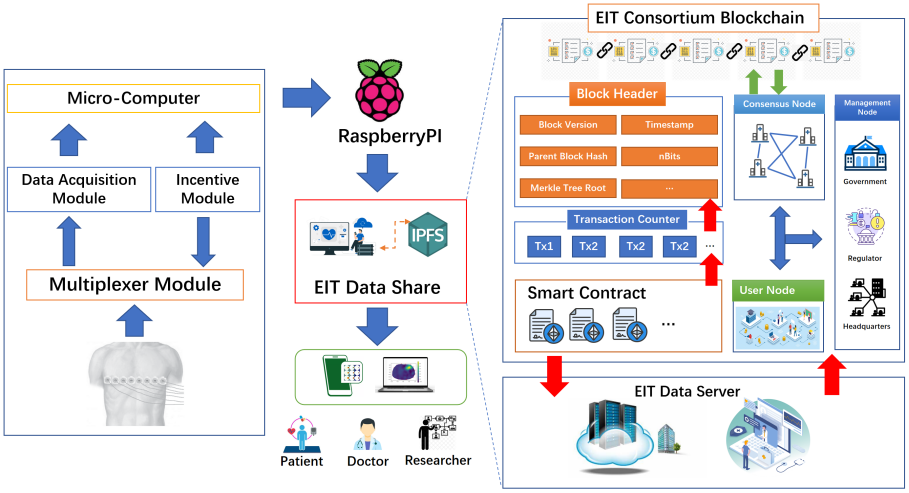

Figure 2. The framework of the remote EIT image-reconstruction system.

(1) This chapter examines the use of EIT systems for remote non-invasive lung and brain imaging and diagnostic applications. The data collection system is compact and portable, making it suitable for emergency situations such as traffic accidents and natural disasters. It can measure voltage data from the human body, which are then transmitted wirelessly to the cloud. The cloud server reads the data and performs calculations and image reconstruction. The resulting images are then transferred to a mobile device for observation. To ensure a safe current for the human body (below 10 mA), a high-precision constant current source is required to generate the appropriate current signal. A signal generator is also needed to provide an input signal to the current source circuit. The STM 32 processor controls the electrode array, allowing the current signal to be applied to the object being measured according to specific rules. The voltage signal at the boundary is automatically measured in a cyclic manner. Since the voltage change corresponding to the conductivity change is very small, amplification of the voltage signal is necessary for observation and processing. However, amplifying the signal also amplifies the noise, so a filter is added after amplification to remove the noise. The filtered signal is then input into the phase-sensitive demodulation circuit to obtain the real part signal, and a filter is used to extract the DC component. Finally, the analog signal is converted into a digital signal through A/D conversion and uploaded to the cloud via the wireless module.

(2) EIT Consortium Blockchain: The following three categories of nodes make up the consortium blockchain network.

User Node (U): Users who request data and hold ownership are $U_n s$. Individuals with EMRs who are willing to give access to other system users, such as individuals receiving care, are considered data holders. Individuals looking to view EMRs must complete a formal request to the data holders, also referred to as data seekers. Usually, health insurers or researchers are the entities seeking data. Depending on the context, U_n might function as either the requester or the owner of data. Each M_n has the ability to access and synchronize blockchain information.

Consensus Node (L_c): The nodes participating in the consensus procedure are referred to as C_n. They play a key role in generating and validating blocks and data. C_n are primarily responsible for registering U_n identities and monitoring conditions. These entities typically include respected institutions such as research centers, major healthcare facilities, and medical departments at universities. In the consensus algorithm, C_n are divided into two functions: leader and follower.

Management Node (M_n): The medical alliance organization or government agency responsible for healthcare often owns M_n. It is in charge of managing the identification data of U_n and carrying out supervisory responsibilities.

(3) EIT Data Server (EITDS): Acting as a semi-trusted third party, EITDS is primarily responsible for the storage of EMRs.

In this approach, the M_n initially generates the public system parameters. The M_n, along with the C_ns and CS (Cloud Server), independently chooses their private keys and computes their corresponding public keys. When a U_n joins the system, it must select a random number to mask its true identity, creating identity protection data. Subsequently, the U_n shares this random number with all C_ns, utilizing the Shamir secret sharing scheme. Each C_n must verify the shared number it receives. Upon successful verification, the C_n sends a confirmation message to the M_n. After collecting all confirmations, the M_n calculates and sends the pseudo identity back to the U_n. Simultaneously, the M_n links the U_n's identity protection data to the pseudonym as tracking data and records them on the blockchain.

3.2. Security Requirements

In order to ensure the privacy of EIT data holders and maintain secure data sharing between data holders and requesters, a secure EIT data sharing solution must fulfill the following requirements:

(1) Protection of identity privacy: EIT data often contain sensitive personal information, and users prefer to keep their identities confidential. Hence, the solution should safeguard the privacy of users' identities.
(2) Conditional identity tracking: In case of security incidents like unauthorized access, the system may need to track and identify the culprits to prevent further threats. Hence, the proposed solution should incorporate a method for selectively monitoring the genuine identities of malicious users.
(3) Collusion attack prevention: As a proxy node, the consensus group leader is a semi-trusted entity who can collaborate with data requesters and potentially access EIT data without authorization. As a result, any solution implemented should be specifically crafted to prevent collusion between proxy nodes and requesters.
(4) Recovery of user keys: User key recovery is a crucial aspect of EITDS, as the loss of private keys can occur for diverse reasons, such as a lost device, malware, or a forgotten password. In emergency situations where keys are lost, users should have mechanisms in place to promptly recover their keys through trusted channels, to minimize the impact on imaging. Furthermore, the finite storage capacity of blockchain systems presents a challenge as the EIT data volume grows. Insufficient storage capacity may lead to incomplete or lost data, jeopardizing data security. To tackle this issue and ensure secure storage of EIT data, it is essential to address the limitations of blockchain storage capacity.

4. EIT Data Storage and Sharing Solution

4.1. EIT Hardware Design

In order to accurately detect boundary voltages, such as in the lungs, it is crucial to consider the signal-to-noise ratio of the data acquisition circuit in the EIT system. This ratio is influenced by various factors, including random and nonlinear errors in electronic equipment, measured objects, and the environment, directly impacting the imaging sensitivity. Nonlinear errors, caused by the distributed capacitance between electrodes and ground, and excitation current shunt due to common mode voltage, can significantly affect EIT image quality. Therefore, minimizing the shunting of distributed capacitance and nonlinearity from common-mode voltage is essential for improving brain EIT accuracy. To address this, a bioelectrical impedance data acquisition system was designed, to reduce the impact of distributed capacitance and accurately measure excitation current. This system includes a programmable current source to compensate for distributed capacitance effects and a differential acquisition circuit to enhance common-mode voltage suppression. The system comprises an excitation constant current source for precise frequency and amplitude control, an electrode interface subsystem to minimize distributed capacitance and measure excitation return current through intracranial tissue accurately, and a differential

voltage acquisition circuit to further enhance CMRR. The overall structure of the electrical impedance imaging detection platform is illustrated in Figure 3.

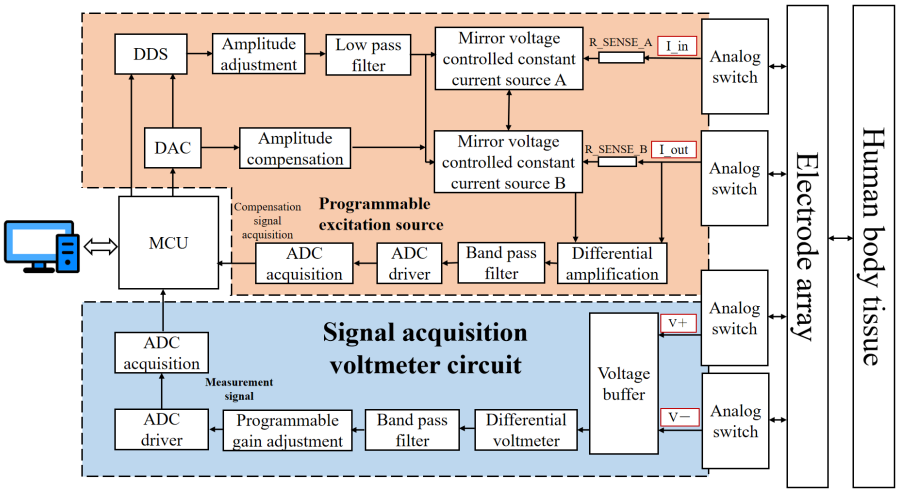

Figure 3. The EIT detection platform structure diagram.

The MCU controls the DDS chip to generate a sinusoidal signal with adjustable frequency. The signal then goes through various circuits such as the amplitude pre-adjustment circuit and spurious frequency filter circuit to output a stable sine wave signal with a set amplitude for driving the mirror voltage. The constant current source is controlled to produce a human body safe excitation current signal that stimulates human tissue, to create a measurable electric field. Simultaneously, the mirror image voltage size is collected to adjust the output excitation current and ensure it reaches the target area at the desired level. The boundary voltage between electrodes is collected, converted to a digital signal through ADC, preprocessed by the main controller, and sent to a PC for numerical calculations and image reconstruction using inverse problem algorithms.

4.2. Initialization

(1) Initialization

We denote k as a system security parameter. And then, the management node M_n chooses a cyclic group G_1 with a prime number order q. The generators g_1 and g_1 are represented in G_1, with a bilinear map denoted as $E : G_1 \times G_1 \to G_n$. Furthermore, M_n picks 8 hash functions that resist collisions.

$$\begin{cases} \text{Hash}_1 : G_1 \to \{0,1\}^* \\ \text{Hash}_2 : \{0,1\}^* \to \mathbb{R}_q^* \\ \text{Hash}_3 : G_1 \to \mathbb{R}_q^* \\ \text{Hash}_4 : G_1 \to G_1 \\ \text{Hash}_5 : R_q^* \to G_1 \\ \text{Hash}_6 : G_1 \times G_1 \to \mathbb{R}_q^* \\ \text{Hash}_7 : G_T \times \{0,1\}^* \times \mathbb{R}_q^* \to \mathbb{R}_q^* \\ \text{Hash}_8 : G_1 \times G_1 \times G_1 \times G_1 \times G_1 \times G_1 \to \mathbb{R}_q^* \end{cases} \tag{1}$$

M_n randomly chooses the private key $PrK_{mn} \in \mathbb{R}_q^*$ and computes the corresponding public key $PubK_{mn} = g_1^{PrK_{mn}}$. The L_c randomly selects private key $PrK_c \in \mathbb{R}_q^*$ and calculates public key $PubK_c = {g_1}^{PrK_c}$, $1 \leqslant c \leqslant n$, with a specified threshold of τ. If L_d denotes the leader in the consensus group, PrK_d is the leader's private key, and the public key is $PubK_d$. User U chooses a strong signature scheme $F = (\text{SigGen}, \text{Verify})$ [36].

Eventually, the system parameters $\{\kappa, G_1, G_2, g_1, g_2, q, e, \text{Hash}_1, \ldots, \text{Hash}_8, PubK_{mn}, n\}$ are revealed by M_n. Then, M_n randomly picks $p_{1,i} \in \mathbb{R}_q^*$ to compute $P_{1,i} = g_1^{P_{1,i}}$ and derive

the protected identity data $\pi_i = Hash_1(P_{1,i}) \oplus Info_i$ for U_i. Following this, M_n randomly chooses a pair of numbers α_i, β_i from $\mathbb{R}_q^*$, to calculate the pseudo-identity $Pseu_i$ and generate the signature σ_i for U_i using the equations below.

$$\begin{cases} z_i = \alpha_i(\beta_i + \mathrm{Hash}_2(\pi_i)) \bmod q \\ \mathrm{Pse}_i = g_1 z_i \\ \delta_i = \mathrm{Hash}_3(\mathrm{Pse}_i) \\ \sigma_i = (z_i + \delta_i PrK_{mn}) \bmod q \end{cases} \tag{2}$$

Upon reception of the identity details $\{Pseu_i, \sigma_i\}$ from M_n, user U_i calculates $\delta^* = Hash_3(Pseu_i)$ to authenticate the validity of the given equation. If the authentication process is successful, U_i adopts $\{Pseu_i, \sigma_i\}$ as his pseudo-identity.

$$g_1^{\sigma_i} = (PubK_{mn})^{\delta^*} \times Pseu_i \tag{3}$$

U_i randomly selects a number a_i from the set $\mathbb{R}_q^*$, then calculates $s_{2,i}$ as $P_{1,i}$ minus a_i. Next, $S_{2,i}$ is generated as $g_1^{s_{2,i}}$ to derive both the private key $PrK_i = Hash_3(S_{2,i})$ and the public key $PubK_i = Hash_4(Pseu_i)^{PrK_i}$. Subsequently, U_i computes A_i as ${g_1}^{a_i}$, produces the signature $\mathrm{sig}_{A,i}$ using the F.Sign signature algorithm, and stores $\{a_i, A_i, sig_{A,i}\}$.

Subsequently, user U_i obtains the public random number λ in $\mathbb{R}_q^*$ given by the present leader via the VRF mechanism and autonomously produces a random number K_i in $\mathbb{R}_q^*$ for computation.

$$\begin{cases} K_i = g_1^{k_i} \\ \lambda_i = \mathrm{Hash}_5(\lambda)^{\mathrm{PrK}_i} \\ \delta_{\lambda,i} = \mathrm{Hash}_2((\mathrm{Pse}_i \| K_i) \| \lambda_i) \\ \sigma_{\lambda,i} = (\lambda + \delta_{\lambda,i}\,\mathrm{PrK}_i) \bmod q \end{cases} \tag{4}$$

Generate basic information about the current self $\{Pseu_i, \sigma_i, K_i, \lambda_i, \sigma_{\lambda,i}\}$.

(2) Encryption

The randomly selected $\varphi \in \{0,1\}^*$ is encrypted by the user U_i to protect the EIT data M_n.

$$\begin{cases} \mathrm{Dec} = E(\mathrm{Hash}_4(Pse_i), \mathrm{Hash}_5(\lambda)^{a_i}) \\ \mathrm{CEIT}_1 = (m \| \varphi) \oplus Dec^{\mathrm{Hash}_6(Pse_i \| PubK_i)} \\ \mathrm{CEIT}_2 = \mathrm{Hash}_4(\mathrm{Pse}_i)^u \\ \mathrm{CEIT}_3 = (\lambda + \mathrm{PrK}_i\,\mathrm{Hash}_7((\mathrm{Dec} \| CEIT_1) \| CEIT_2)) \bmod q \end{cases} \tag{5}$$

Then, the user sends the encrypted data $\{Dec, CEIT_1, CEIT_2, CEIT_3\}$ to the IPFS.

(3) Storage Phase

Upon receiving $\{Dec, CEIT_1, CEIT_2, CEIT_3\}$ from user U_i, the IPFS first conducts verification.

$$Hash_4(Pseu_i)^{CEIT_3} = CEIT_2 \times PubK_i^{Hash_7((Dec \| CEIT_1) \| CEIT_2)} \tag{6}$$

If the successful validation demonstrates that the confidentiality, integrity, and source of the encrypted data remain intact, the IPFS will store $\{Dec, CEIT_1, CEIT_2, CEIT_3\}$ and generate the download link for ciphertext of U_i.

In order to minimize the storage burden on the blockchain, U_i submits a request to upload its metadata onto the blockchain. The metadata contains the URL, the hash value h_m of message data M_n, and the $Pseu_i$ of U_i.

After completing the block upload, the subsequent leader L_d is determined using a randomly generated number through the verifiable random function VRF, following $L = (\theta \bmod N) + 1$. The process for this procedure are elaborated below. The current leader creates a random θ and proof p using its private key PrK and the current timestamp x. These parameters $\{\theta, p\}$ are then publicly disclosed by the leader. The authenticity of θ

can be confirmed by the other follower nodes through validation using the public key vk of the leader, the current timestamp x, the pseudo-random string θ, and the proof p.

The consensus group determines $L = (\theta \bmod N) + 1$ and designates L_d as the leader after all nodes have been verified. This selection is predicated on the VRF function's arbitrary output value, which ensures impartiality and unpredictability in the voting process.

(4) Requests, authorizations, and visits

If U_i wants to access U_j's data information M_n, U_i must obtain permission from U_j.

U_i requests access to U_j's data and transmits essential details $\{PID_i, \sigma_i, K_i, u_i, \sigma_{u,i}\}$. U_j validates the identity of U_i using Equation (1) and subsequently authenticates the parameters of U_i.

$$Hash_4\left(PID_j\right)^{\sigma_{u,j}} = \left(PubK_j\right)^{Hash_2\left(\left(PID_j \| K_j\right) \| u_j\right)} \times Hash_4\left(PID_j\right)^{u} \tag{7}$$

If the equation mentioned above is satisfied, the authentication will be successful. U_j is permitted by U_i to retrieve the required information.

$$\begin{cases} d_j = PID_j \times \left(\mathrm{PubK}_{mn}\right)^{\mathrm{Hash}_3\left(PID_j\right)}\Big) \\ rk_1 = \mathrm{Hash}_8\Big(\left(d_j k_i \Big\| K_j^{\sigma_i}\right) \Big\| \left(PID_i \| PID_j\right) \| \left(PubK_i \| PubK_j\right)\Big) \\ rk_2 = \left(u_j\right)^{\frac{a_i}{PrK_i}} \\ r_{i\to j} = \{rk_1, rk_2\} \end{cases} \tag{8}$$

The re-encryption key $r_{i\to j}$ is created by user U_i, who then uses F.Sign to generate the signature sig_r on $r_{i\to j}$ before sending $\left\{r_{i\to j}, sig_r\right\}$ to the agent node.

(5) Proxy Re-encryption

The agent node holds a private key PrK_L and a public key $PubK_L$ as the leader. When $\left\{r_{i\to j}, sig_r\right\}$ is received, the agent node uses the F.SignVerif algorithm for verification. Upon signature verification, the node agent retrieves the encrypted data $\{Dec, CEIT_1, CEIT_2, CEIT_3\}$ from the IPFS and authenticates it utilizing Equation (6). In the event of a successful validation, the encrypted data undergo re-encryption via a predefined algorithm.

$$\begin{cases} \mathrm{Dec}' = E(\mathrm{PubK}_i, rk_2) \\ \mathrm{CEIT}_1{}' = \mathrm{CEIT}_1{}^{rk_1} \\ \mathrm{CEIT}_2{}' = g_1{}^{u} \\ \mathrm{CEIT}_3{}' = \left(u + \mathrm{PrK}_L\, \mathrm{Hash}_7\left(\left(\mathrm{Dec}' \| \mathrm{CEIT}_1{}'\right) \| \mathrm{CEIT}_2{}'\right)\right) \bmod q \end{cases} \tag{9}$$

The newly encrypted ciphertext $\left\{Dec', CEIT_1{}', CEIT_2{}', CEIT_3{}'\right\}$, can be acquired and sent to U_j.

(6) Decryption

The ciphertext $\{Dec, CEIT_1, CEIT_2, CEIT_3\}$ derived from the IPFS by user U_i is verified using Equation (2). Once successfully verified, the ciphertext will be decrypted by the equations, as follows:

$$\begin{cases} \mathrm{Dec} = E(\mathrm{Hash}_4(\mathrm{Pse}_i), \mathrm{Hash}_5(u)^{a_i}) \\ m \| \varphi = CEIT_1 \oplus D^{\mathrm{Hash}_6(\mathrm{Pse}_i \| PubK_i)} \end{cases} \tag{10}$$

After receipt of the re-encrypted ciphertext $\left\{Dec', CEIT_1{}', CEIT_2{}', CEIT_3{}'\right\}$, U_j proceeds to verify it using the equation below:

$$g_1{}^{CEIT_3{}'} = CEIT_2{}' \times PubK_L{}^{Hash_7\left(\left(Dec' \| CEIT_1{}'\right) \| CEIT_2{}'\right)} \tag{11}$$

Upon successful verification, U_j uses the formulas below to decrypt the re-encrypted ciphertext:

$$\begin{cases} d_i = \mathrm{Pse}_i \times (\mathrm{PubK}_{mn})^{\mathrm{Hash}_3(\mathrm{Pse}_i)} \\ rk_1 = \mathrm{Hash}_8\left((K_i^{\sigma_j} \| d_i^{k_j}) \| PID_i \| PID_j \| PubK_i \| PubK_j\right) \\ CEIT_1 = (CEIT_1)^{\frac{1}{rk_1}} = (m \| \varphi) \oplus \mathrm{Dec}^{\mathrm{Hash}_6(\mathrm{Pse}_i \| PubK_i)} \\ \mathrm{Dec}' = \left(\mathrm{Dec}'\right)^{\frac{1}{\mathrm{PrK}_j}} \\ m \| \varphi = CEIT_1 \oplus \mathrm{Dec}^{\mathrm{Hash}_6(\mathrm{Pse}_i \| PubK_i)} \end{cases} \tag{12}$$

(7) Traceability

Utilizing a clandestine method of distribution, this research employs $\tau - 1$ random numbers $a_{1,i}, \ldots, a_{\tau-1,i}$ chosen by M from the set R_q^* to achieve the trackability of fictitious identities. This allows the sharing of $P_{1,i}$ and the generation of a polynomial with a degree of $(\tau - 1)$:

$$F_i(x) = a_{0,i} + a_{1,i}x + a_{2,i}x^2 + \cdots + a_{\tau-1,i}x^{\tau-1} \bmod q \tag{13}$$

The polynomial shares $\{F_i(1), F_i(2), \cdots, F_i(n)\}$ and polynomial commitments shares $\langle \Lambda_c \rangle_{c=1\sim n}$ are calculated by $a_{0,i} = s_{i,1}$:

$$\Lambda_c = PubK_c{}^{F_i(c)}, 1 \leqslant c \leqslant n \tag{14}$$

In order to confirm the polynomial share distribution in the subsequent steps, M must calculate the polynomial parameters commitments $\langle C_\delta \rangle_{\delta=0\sim\tau-1}$:

$$C_\delta = g_2{}^{a_{l,i}}, 0 \leqslant \delta < \tau - 1 \tag{15}$$

for all polynomials commitments $\langle \Phi_c \rangle_{c=1\sim n}$:

$$\Phi_c = g_2{}^{F_i(c)}, 1 \leqslant c \leqslant n \tag{16}$$

Then, we begin to verify whether $F_i(c)$ in Φ_c is the result of polynomial $F_i(x)$ created by M, and L_c needs to confirm the validity of the following equation [37]:

$$\Phi_c = \prod_{\delta=0}^{\tau-1} (C_\delta)^{c^\delta} \tag{17}$$

Next, L_c calculates: $R_c = E(\Phi_c, PubK_c), 1 \leqslant c \leqslant n$ and utilizes the subsequent method for bulk verification:

$$\prod_{c=1}^{n} \Gamma_c = E\left(g_2, \prod_{c=1}^{n} \Lambda_c\right) \tag{18}$$

If the equation stated above is valid, L_c affirms the accuracy of all polynomial commitments $\langle \Lambda_c \rangle_{c=1\sim n}$ that have been received and retains the associated $\{\pi_i, \Lambda_c\}$. Every L_c then employs its individual private key PrK_c to retrieve Shr_c from Λ_c.

$$\mathrm{Shr}_c = (\Lambda_c)^{\frac{1}{PrK_c}} \tag{19}$$

In order to verify the authenticity of the Shr_c transmitted by N_c, proof information must be provided by L_c to ensure that recipients are indeed receiving Shr_c from the corresponding Λ_c. To begin, L_c randomly chooses a number r_c from the set R_q^* and computes $B_{c,1} = (Shr_c)^{r_c}$ along with $B_{c,2} = (g_1)^{r_c}$. Subsequently, L_c performs the following calculations:

$$e_c = Hash_2(Shr_c \| g_1 \| \Lambda_c \| PubK_c \| B_{1,c} \| B_{2,c}), b_c = r_c + e_c PrK_c \tag{20}$$

and ultimately produces shared information $\{Shr_c, e_c, b_c\}$ that can be employed for identifying traces and regaining keys.

The user $\{\pi_i, Pseu_i\}$ has traceability information logged by M by initiating an on-chain request, which allows the consensus group to track down any dishonest users. A smart contract is used to automatically track down the rogue node. When a user exhibits malicious conduct, the tracing procedure is initiated automatically when the threshold τ is exceeded by the number of L_c that deems the user malicious. The precise steps for tracking are as follows:

Every L_c sends its tracing $\{Shr_c, e_c, b_c\}$ to the smart contract. When τ is reached in the quantity of tracing Shr given to the contract, the smart contract will retrieve the user's $P_{1,i}$ by executing the tracing technique described in Algorithm 1. Finally, the group consensus will reveal the true identity information Info_i of user U_i using the following equation:

$$Info_c = \pi_c \oplus Hash_1(P_{1,c}) \tag{21}$$

Algorithm 1 The algorithm for tracking the malicious nodes.

Input:
$\pi_i, [Shr_1, Shr_2, \ldots, Shr_t], [e_1, e_2, \ldots, e_t], [b_1, b_2, \ldots, b_t]$
Output:
$\pi_i \oplus Hash_1(P_{1,i})$
for $c = 1$ to τ do
  Calculate:
  temporary $= (Shr_c \| g_1) \| (\Lambda_c \| pk_c) \| (\text{Shr}_c)^{b_c} (\Lambda_c)^{-e_c} \| {g_1}^{b_c} (\Lambda_c)^{-e_c}$
  ${e_c}^* = Hash_2(temp)$
  if ${e_c}^* \neq e_c$ then
    fail
  end if
end for
$P_{1,c} = 1$
for $c = 1$ to τ do
  $\prod_{j=1, j\neq c}^{t} \frac{j}{j-c} = 1$
  for $j \in [1, t]$ do
    if $j \neq c$ then
      $\prod_{j=1, j\neq c}^{\tau} \frac{j}{j-c} = \prod_{j=1, j\neq c}^{\tau} \frac{j}{j-c} \times \frac{j}{j-c}$
    end if
  end for
  $P_{1,c} = P_{1,c} \times pow(\text{Shr}_c, \prod_{j=1, j\neq c}^{\tau} \frac{j}{j-c})$
end for

5. Theoretical Analysis

5.1. Correctness Analysis of the Scheme

Theorem 1. *This paper's proposed EITDS scheme is accurate.*

Proof. Demonstrating the proposed EITDS scheme's correctness requires showing that equations in (3)–(6) are satisfied.

(1) In the case of the identity data $\{Pseu_i, \sigma_i\}$, if the calculated value of δ^* is the same as τ_i, then the following holds:

$${g_1}^{\sigma_i} = g_1^{(z_i + \tau_i \tau k_{mn})} = (PubK_{mn})^{\tau^*} \times Pseu_i \tag{22}$$

Therefore, Equation (3) holds.

(2) The ciphertext $\{Dec, CEIT_1, CEIT_2, CEIT_3\}$ satisfies Equation (6).

$$\begin{aligned} Hash_4(PID_1)^{CEIT_3} &= Hash_4(Pseu_i)^{(u+PrK_1 Hash_7(Dec,CEIT_1,CEIT_2))} \\ &= CEIT_2 \times PubK_i^{Hash_7(Dec,CEIT_1,CEIT_2)} \end{aligned} \tag{23}$$

(3) The $rk_1 = Hash_8\left(d_j^{k_i} \middle\| K_j^{\sigma_i} \middle\| Pseu_i \middle\| PID_j \middle\| PubK_i \| PubK_j\right)$ used by U_i for encryption satisfies Equation (8).

$$\begin{aligned} rk_1 &= Hash_8\left(d_j^{k_i} \middle\| K_j^{\sigma_i} \middle\| Pseu_i \middle\| PID_j \middle\| PubK_i \| PubK_j\right) \\ &= H_s\left(\left(PID_j \times (PubK_{mn})^{Hash_3(PID_j)}\right)^{k_i} \| \left(g_1^{k_j} \sigma^{\sigma_i} \| Pseu_i \| PID_j \| PubK_i \| PubK_j\right)\right. \\ &= Hash_8\left(K_i^{2+PrK_{\infty n} Hash_3(PID_j)} \middle\| g_1^{k_i(x_i+PrK_{mn} H_s\langle Pseu_i\rangle)\}} \middle\| Pseu_i \middle\| PID_j \middle\| PubK_i \| PubK_j\right) \\ &= Hash_8\left(K_i^{\sigma_j} \middle\| d_i^{k_j} \middle\| Pseu_i \middle\| PID_j \middle\| PubK_i \| PubK_j\right) \end{aligned} \tag{24}$$

(4) The commitments $\langle C_\delta \rangle_{i=0,-1-1}$ published by U_i can be expressed as follows if the polynomial $f_1(x)$ generates $F_i(c)$ concealed in Φ_c.

$$\prod_{l=0}^{\tau-1} (C_\delta)^{\mathrm{t}^{\mathrm{t}}} = \prod_{\delta=0}^{\tau-1} (g_2)^{n_1, c^\delta} = g_2 \sum_{j=0}^{\sum_{j=0}^{\tau-1} a_\delta + c^\delta} = g_2{}^{F_i(c)} = \Phi_c \tag{25}$$

Therefore, Equation (17) holds.

(5) When the $\{\langle \Phi_c \rangle_{c=1\sim n}, \langle \Gamma_c \rangle_{c=1\sim n}\}$ is made available to the public, and assuming the $\langle \Lambda_c \rangle_{c=1\sim n}$ are accurate, we can conclude the following:

$$\begin{aligned} \prod_{c=1}^{n} \Gamma_c &= \prod_{c=1}^{n} e(\Phi_c, PubK_c) = \prod_{c=1}^{n} e\left(g_2{}^f(c), PubK_c\right) = \prod_{c=1}^{n} e(g_2, Y_i) \\ &= e(g_2, Y_1 \cdot Y_2 \cdots Y_n) = e\left(g_2, \prod_{c=1}^{n} \Lambda_c\right) \end{aligned} \tag{26}$$

Therefore, Equation (18) holds.

$$\prod_{c=1}^{\tau} (\mathrm{Shr}_c)^{L_c} = \prod_{c=1}^{\tau} \left((\Lambda_c)^{\frac{1}{sk_c}}\right)^{L_c} = \prod_{c=1}^{\tau} \left(g_1{}^{f_i(c)}\right)^{L_c} \tag{27}$$

Then, let $\xi = \sum_{c=1}^{\tau} \left(f_i(c) \prod_{j=1, j\neq c}^{\tau} \frac{j}{j-c}\right)$.

So, we can obtain

$$\prod_{c=1}^{\tau} (\mathrm{Shr}_c)^{L_c} = g_1{}^{\xi} = g_1{}^{f_i(0)} = P_{1,i} \tag{28}$$

τ or more correctly Shr_c with $P_{1,i}$ satisfy the equation above. □

5.2. Security Analysis of the Scheme

Theorem 2. *A secure method for maintaining identity privacy with anonymity and traceability in a distributed setting is guaranteed if the DL and CDH assumptions are met.*

Proof. Within this system for safeguarding identity privacy, three methods exist for an intruder to access the individual's actual identity details:

If the adversary successfully uncovers exposed shared e_c through the utilization of the disclosed data $\{g_1, g_2, \Phi_c, \Lambda_c, PubK_c\}$, upon securing τ instances of share, the adversary will then proceed to regain $S_{1,}$ and determine info through π_i.

To make the proof simpler, let $g_1 = g_2{}^{\alpha}$, $\Phi_c = g_2{}^{F_i(c)} = g_2{}^{\beta}$, $PubK_c = g_1{}^{PrK_c} = g_2{}^{\alpha PrK_c} = g_2^{\gamma}$, and consequently we obtain $\Lambda_c = PubK_c{}^{fi(c)} = g_2{}^{\beta\gamma}$. The adversary's goal is

to acquire share $c_c = {g_1}^{F_i(c)} = {g_2}^{\alpha F_i(c)} = {g_2}^{\alpha\beta}$. Therefore, the task changes to calculating ${g_2}^{\beta\alpha}$, with ${g_2}^{\beta}, {g_2}^{\gamma}$, and ${g_2}^{\beta}\gamma$ given, for any $\alpha, \beta, \gamma \in R_q^*$. A potential attacker, armed with all available public information, could attempt to compute ${g_2}^{\alpha\beta}$ using two distinct approaches:

(1) The attacker may try to calculate ${g_2}^{\alpha\beta}$ directly using ${g_2}^{\alpha}$ and ${g_2}^{\beta}$. Based on the assumption of CDH, it is impossible for any probabilistic polynomial-time attacker to efficiently calculate ${g_2}^{\alpha\beta}$ given $g_2, {g_2}^{\alpha}$, and ${g_2}^{\beta}$, where $\alpha, \beta \in R_q^*$. Consequently, this approach contradicts the CDH assumption.

The adversary might attempt to compute β from ${g_2}^{\gamma}$ and ${g_2}^{\beta\gamma}$. Nonetheless, according to the DL hypothesis, in the presence of g_2^{γ} and ${g_2}^{\beta\gamma}$, for any $\gamma \in R_q^*$, there is no chance of a computational adversary working in polynomial time determining β with a significant advantage. Hence, without access to β, it is not feasible to proceed with the computation of ${g_2}^{\alpha\beta}$.

To summarize, with the assumptions of DL and CDH, the attacker is prevented from acquiring share c_c solely through the public information. This means that the attacker is incapable of gathering sufficient shares to retrieve $P_{1,i}$ and subsequently calculate information.

The adversary has the ability to eliminate up to $\tau - 1 N_c$. From there, they can access the $\langle PrK_c \rangle_{c=1\sim\tau-1}$ and $\langle$ share $_c\rangle_{c=1\sim\tau-1}$. An attempt may be made by the adversary to retrieve the $P_{1,i}$ and $Info_i$ of U_i using $\{\langle PrK_c \rangle_{c=1\sim\tau-1}, \langle \text{ Shr } \rangle_{c=1\sim\tau-1}\}$ along with other publicly available details $\{\langle \Phi_c \rangle_{c=1\sim n}, \langle \Lambda_c \rangle_{c=1\sim n}, \langle PubK_c \rangle_{c=1\sim n}, \langle C_\delta \rangle_{\delta=0\sim\tau-1}\}$.

If $g_1 = g_2^{\alpha}$ and $C_0 = {g_2}^{\alpha_{0,i}} = {g_2}^{P_{1,i}} = {g_2}^{\beta}$, then the opponent's objective is to determine β or ${g_2}^{\alpha\beta}$. Using the available information, the adversary could aim to compute either β or ${g_2}^{\beta\alpha}$ from three different perspectives:

(2) The adversary could explore the calculation of β from $C_0 = {g_2}^{\beta}$, which is tantamount to addressing the issue of DL. Consequently, this challenges the DL assumption.

The adversary might attempt to calculate ${g_2}^{\alpha\beta}$ using ${g_2}^{\alpha}$ and $C_0 = {g_2}^{\beta}$. Yet, this approach is analogous to addressing the CDH dilemma, thus conflicting with the CDH hypothesis.

(3) Potential adversary strategy: $\langle \text{Shr}_c \rangle_{c=1\sim\tau-1}$ could be used to extract $g_2^{\alpha\beta}$. Nevertheless, if at least τ shares or more of quantity c are gathered, the opponent can only obtain ${g_2}^{\alpha\beta}$, according to the interpolation Lagrange theorem.

$$\prod_{c=1}^{\tau} (\text{Shr}_c)^{f_c} = \prod_{c=1}^{\tau} (g_1 F_i(c))^{L_0} = {g_1}^{\sum_{c=1}^{e} F_i(c) L_o} = g_1 F_i(0) = {g_2}^{s_{1,i}} = {g_2}^{\alpha\beta} \tag{29}$$

$$f_c = \prod_{j=1, j\neq c}^{\tau} \frac{j}{j-c} \tag{30}$$

However, the adversary only has a maximum of $\tau - 1$ duplicates of share c, making it impossible to retrieve $P_{1,i}$ or $P_{1,i}$ from them. Furthermore, the opponent and the compromised L_c can try to use their existing data to decrypt the remaining $\langle \text{Shr}_c \rangle_{c=t\sim n}$ to meet the threshold τ. However, based on the assumptions of DL and CDH, we have shown that an adversary cannot obtain shares of the pure L_c using publicly available information.

In conclusion, the attacker cannot reassemble $P_{1,i}$ and $Info_i$ with the corruption of $\tau - 1$ or less L_c, as long as the DL and CDH assumptions are satisfied.

The attacker makes a determined effort to decipher the secret data in $Info_i$ using public identity protection information π_i.

$$\prod_{c=1}^{t} (\text{Shr}_c)^{L_c} = P_{1,c}, \text{Info}_c = \pi_c \oplus Hash_1(P_{1,c}) \tag{31}$$

In order to safeguard the true identity of U_i, M creates identity protection data $\pi_i = Hash_1(P_{1,i}) \oplus Info_i$ specifically for U_i. Based on the preceding context, it is infeasible for

any attacker to retrieve $P_{1,i}$. Furthermore, with a sufficiently robust security parameter κ, it becomes challenging to illicitly decipher the genuine identity data info from the protection data π_i. Hence, given a reasonable level of security strength, the adversary is unable to expose info from π_i".

Overall, the suggested mechanism for safeguarding identity privacy with anonymity and traceability is reliable. Only when τ or more consensus nodes detect malicious actions by the user will their true identity be exposed. □

Theorem 3. *The data's confidentiality is guaranteed by this scheme.*

Proof. The core of the EITDS data-sharing mechanism is the proposed privacy-preserving encryption (PRE) technique, which guarantees the confidentiality of data during transport. Once authorized by the data owner, a new re-encryption key is generated for the receiver and transmitted to the intermediary node L_c. Subsequently, the intermediary node L_c utilizes the re-encryption key to modify the encrypted data, enabling the recipient to decrypt the altered data with their corresponding key. Importantly, throughout this process, the intermediary node strictly manages the re-encryption key from U_i and manipulates the encrypted data without accessing any sensitive information from the original or modified data. Ultimately, this approach effectively safeguards data confidentiality. □

Theorem 4. *This scheme can withstand collusion attempts.*

Proof. The leader selected from the group N_c is referred to as L_N. This leader is chosen using the equation $L = (\text{num} \bmod n) + 1$. Subsequently, L_N issues a randomly generated encryption key u to ensure data security. If L_1 stores the random value $u^{(1)}$ in a block at height $Hash_1$ and logs containing information m_1 in the same block, a data requester U_j must combine $u^{(1)}$ with their personal key PrK_j to calculate $u_j = Hash_5(u)^{PrK_j}$ in order to access data linked to said block. Once u_j is calculated, U_j forwards an access request to U_i with the derived data u_j. If U_i approves the retrieval of m_1, U_j needs to create a new encrypted key $rk_{i\to j} = \left(u_j^{(1)}\right)^{a_i/PrK_i}$ using u_j and their private key PrK_i, and then send it to the intermediary node.

The group in agreement will vote for Leader L_c, the new leader, in accordance with the rules, after the current agreement expires. Additionally, at $Hash_2$, the metadata of m_2 and the random number $u^{(2)}$ generated by Leader_2 are both recorded in a block. During the encryption step, the following equations are utilized by U_i to encrypt m_2:

$$\begin{cases} \text{Dec}^{(2)} = E\left(\text{Hash}_4(\text{ Pse }_i), \left(u_i^{(2)}\right)^{a_4}\right) \\ \text{CEIT}_1{}^{(2)} = (m_2 \| \varphi) \oplus \left(\text{Dec}^{(2)}\right)^{\text{Hash }_6(P_{se}e_i \| PubK_i)} \\ \text{CEIT}_2^{(2)} = \text{Hash}_4(\text{ Pse }_i)^{\left(u^{(2)}\right)} \\ \text{CEIT}_3{}^{(2)} = \left(u^{(2)} + \text{PrK}_i \, \text{Hash}_7\left(\text{Dec}^{(2)} \left\| CEIT_1^{(2)} \right\| CEIT_2^{(2)}\right)\right) \bmod q \end{cases} \tag{32}$$

The proxy node can only obtain $\left(Hash_5\left(u^{(1)}\right)\right)^{a_i/PrK_i}$ in relation to the previous random number $u^{(1)}$ if it conspires with U_j to gain unauthorized access to m_2. They can then compute $E\left(pk_i, \left(Hash_5\left(u^{(1)}\right)\right)^{a_i/PrK_i}\right) = E\left(Hash_4(PID_i), Hash_5\left(u^{(1)}\right)\right)^{a_i}$. This is ineffective for accessing m_2, though, in contrast to $Dec^{(2)} = e\left(Hash_4(PID_i), Hash_5\left(u^{(2)}\right)\right)^{a_i}$. This is also true for other types of data. As a result, this method successfully prevents the proxy node and data requesters from cooperating. □

6. Complexity and Experimental Analysis

6.1. Complexity Analysis

In Table 2, we analyzed the computation costs of encryption, generation of re-encryption keys, re-encryption, self-decryption, and re-decryption within our approach compared to the existing literature. Our emphasis was on examining the most time-intensive tasks in these stages, including exponentiations within group G_1 and bilinear pairing e. The time taken for an exponentiation in G_1 and a bilinear pairing operation is denoted as Exp and Pair, respectively.

Table 2. Comparison of different types of blockchains.

Scheme	[38]	[39]	[40]	[41]	Ours
Encrypt	2Exp + 2Pair	8Exp	4Exp	3Exp + 1Pair	3Exp + 1Pair
ReKeyGen	2Exp	2Exp	2Exp	5Exp	4Exp
ReEncrypt	1Exp + 1Pair	2Exp + 5Pair	1Exp + 2Pair	2Exp + 4Pair	4Exp + 1Pair
Self-Decrypt	1Pair	3Exp + 3Pair	–	–	4Exp + 1Pair
ReDecrypt	1Exp + 2Pair	2Exp + 2Pair	1Exp + 3Pair	2Exp + 4Pair	8Exp

Our technique showed great computational efficiency throughout the re-encryption and re-decryption operations, based on the computational complexity data presented in Table 2. Moderate computing performance was achieved during the encryption and self-decryption stages. Although re-encryption key creation might not provide a significant benefit, the difference was not great.

6.2. Performance Analysis

A thorough performance simulation and quantitative analysis of the EITDS are given in this section. The evaluation took into account the average number of attempts required for each step: initialization, encryption, re-encryption, self-decryption, and re-decryption in proxy re-encryption. The Go language-based PBC library was used to simulate the system in order to replicate real-world conditions. The experiments were carried out with 64 GB of RAM and a quad-core Xeon processor running Ubuntu 20.04.

According to the data presented in Figure 4, the average time spent on initiation, encoding, re-encoding for essential creation, re-encoding, self-decrypting, and re-decrypting was 7.232 ms, 4.631 ms, 5.118 ms, 5.923 ms, 3.072 ms, and 10.367 ms, respectively. The efficiency of encoding, re-encoding, and self-decrypting in the intermediate re-encryption system seems adequate when considering the time allotted to each step. The marginally increased costs associated with essential re-encryption formation and re-decrypt were mostly attributable to the exponential operations, the execution of which was contingent upon the volume and intricacy of the input data. Based on Figure 5a, our technique performed at a medium level during the encryption stage. However, in the re-encryption stages, our scheme's computational overhead was lowest, as seen in Figure 5b. Based on the comparison above, our technique performed exceptionally well during the encryption and re-encryption phases. All EIT data only needed to be encrypted and saved once, despite our scheme's medium-level performance during the encryption stage. All things considered, this system's computational cost stayed within an acceptable and controllable range.

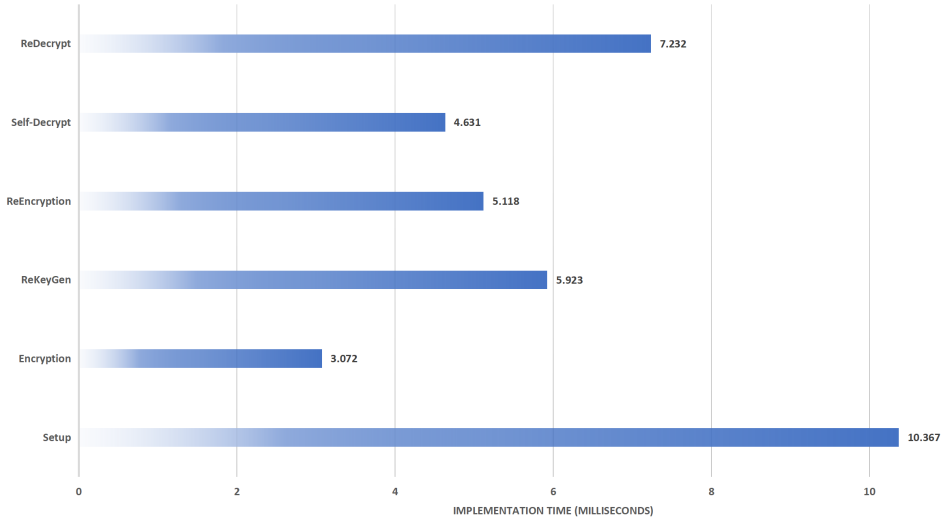

Figure 4. Time consumed by the six stages.

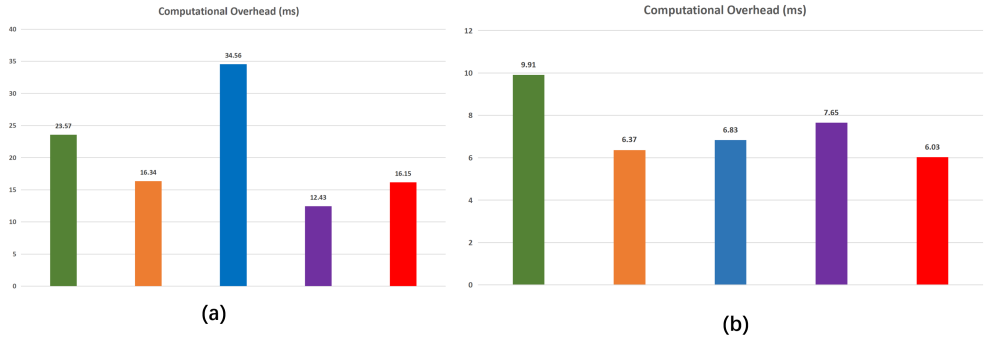

Figure 5. A comparison of various schemes (green indicates [38], yellow indicates [39], blue indicates [40], purple indicates [41], and red indicates our scheme). (**a**) A comparison of the encryption stage's computational overhead. (**b**) A comparison of the re-encryption stage's computational overhead.

7. Conclusions

This paper proposed an EITDS based on consortium blockchain. The EITDS utilizes a portable EIT data collector to enhance data comprehensiveness and timeliness within the system. To address concerns about malicious user identification, while safeguarding data and identity privacy, the EITDS employs PRE data sharing technology, balancing data anonymity and traceability of identity to enable precise data access control. This technology is designed to withstand collusion attacks, preventing semi-trusted agents from collaborating with data requesters to access unauthorized EIT data. Furthermore, the EITDS integrates blockchain and IPFS distributed storage technology to establish a secure collaborative data storage model, both on and off the chain, addressing the challenge of secure storage for large-scale data. The computational complexity and operational performance of the scheme were analyzed through numerical experiments. Proxy re-encryption excelled in the efficiency of encryption, re-encryption, and self-decryption stages when considering the average time consumption. Through safety comparisons, experimental analysis, and exploration of related technologies, the EITDS was demonstrated to be a secure and efficient medical data sharing system suitable for practical applications.

The solution proposed in this article has some shortcomings, including a slightly cumbersome request and authorization process. Future work will focus on streamlining the user operation steps to enhance the user experience, while maintaining safety. Improvements will be made to the encryption and retrieval algorithms to reduce the data request time.

Author Contributions: Conceptualization, R.Z. and C.X.; methodology, R.Z.; software, R.Z.; validation, R.Z., Z.Z. and W.M.; formal analysis, R.Z.; investigation, R.Z.; resources, W.M.; data curation, R.Z.; writing—original draft preparation, R.Z.; writing—review and editing, C.X.; visualization, R.Z.; supervision, W.M. and C.X.; project administration, C.X.; funding acquisition, C.X., Z.Z. and W.M. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China (62171147, 62161008, 62361017), the Guangxi Key Laboratory of Automatic Detecting Technology and Instruments (YQ20113, YQ20114, YQ23015).

Data Availability Statement: The data supporting this study's findings are available upon reasonable request from the corresponding author, xcp@guet.edu.cn.

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

References

1. Li, Z.; Zhang, J.; Liu, D.; Du, J. CT Image-Guided Electrical Impedance Tomography for Medical Imaging. *IEEE Trans. Med. Imaging* **2020**, *39*, 1822–1832. [CrossRef] [PubMed]
2. Adler, A.; Boyle, A. Electrical impedance tomography: Tissue Properties to image measures. *IEEE Trans. Biomed. Eng.* **2017**, *64*, 2494–2504. [PubMed]
3. Newell, J.; Isaacson, D.; Mueller, J. Electrical Impedance Tomography. *IEEE Trans. Med. Imaging* **2002**, *21*, 553–554. [CrossRef]
4. Brown, B. Electrical impedance tomography (EIT): A review. *J. Med. Eng. Technol.* **2003**, *27*, 97–108. [CrossRef] [PubMed]
5. Adler, A.; Arnold, J.H.; Bayford, R.; Borsic, A.; Brown, B.; Dixon, P.; Faes, T.J.; Frerichs, I.; Gagnon, H.; Gärber, Y.; et al. GREIT: A unified approach to 2D linear EIT reconstruction of lung images. *Physiol. Meas.* **2009**, *30*, S35. [CrossRef]
6. Kłosowski, G.; Hoła, A.; Rymarczyk, T.; Mazurek, M.; Niderla, K.; Rzemieniak, M. Using Machine Learning in Electrical Tomography for Building Energy Efficiency through Moisture Detection. *Energies* **2023**, *16*, 1818. [CrossRef]
7. Enaizan, O.; Zaidan, A.A.; Alwi, N.; Zaidan, B.B.; Alsalem, M.A.; Albahri, O.; Albahri, A. Electronic medical record systems: Decision support examination framework for individual, security and privacy concerns using multi-perspective analysis. *Health Technol.* **2020**, *10*, 795–822. [CrossRef]
8. Adamu, J.; Hamzah, R.; Rosli, M.M. Security issues and framework of electronic medical record: A review. *Bull. Electr. Eng. Inform.* **2020**, *9*, 565–572. [CrossRef]
9. Stanfill, M.H.; Marc, D.T. Health information management: Implications of artificial intelligence on healthcare data and information management. *Yearb. Med. Inform.* **2019**, *28*, 056–064. [CrossRef]
10. Xia, Q.; Sifah, E.B.; Smahi, A.; Amofa, S.; Zhang, X. BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments. *Information* **2017**, *8*, 44. [CrossRef]
11. Chen, Y.; Ding, S.; Xu, Z.; Zheng, H.; Yang, S. Blockchain-Based Medical Records Secure Storage and Medical Service Framework. *J. Med. Syst.* **2018**, *43*, 1–9. [CrossRef]
12. Sivan, R.; Zukarnain, Z. Security and Privacy in Cloud-Based E-Health System. *Symmetry* **2021**, *13*, 742. [CrossRef]
13. Amiri, M.J.; Agrawal, D.; El Abbadi, A. Permissioned blockchains: Properties, techniques and applications. In Proceedings of the 2021 International Conference on Management of Data, Virtual Event, 20–25 June 2021; pp. 2813–2820.
14. Chen, Y.; Xie, H.; Lv, K.; Wei, S.; Hu, C. DEPLEST: A blockchain-based privacy-preserving distributed database toward user behaviors in social networks. *Inf. Sci.* **2019**, *501*, 100–117. [CrossRef]
15. Ren, Y.; Leng, Y.; Qi, J.; Sharma, P.K.; Tolba, A. Multiple cloud storage mechanism based on blockchain in smart homes. *Future Gener. Comput. Syst.* **2021**, *115*, 304–313. [CrossRef]
16. Qiao, R.; Luo, X.Y.; Zhu, S.F.; Liu, A.D.; Wang, Q.X. Dynamic Autonomous Cross Consortium Chain Mechanism in e-Healthcare. *IEEE J. Biomed. Health Inform.* **2020**, *24*, 2157–2168. [CrossRef]
17. Wang, Y.; Wang, J.; Chen, X. Secure searchable encryption: A survey. *J. Commun. Inf. Netw.* **2016**, *1*, 52–65. [CrossRef]
18. Xu, M.; Liu, S.; Yu, D.; Cheng, X.; Guo, S.; Yu, J. Cloudchain: A cloud blockchain using shared memory consensus and rdma. *IEEE Trans. Comput.* **2022**, *71*, 3242–3253. [CrossRef]
19. Wu, Y.; Cegielski, C.G.; Hazen, B.T.; Hall, D.J. Cloud computing in support of supply chain information system infrastructure: Understanding when to go to the cloud. *J. Supply Chain Manag.* **2013**, *49*, 25–41. [CrossRef]
20. Liu, X.; Wang, Z.; Jin, C.; Li, F.; Li, G. A blockchain-based medical data sharing and protection scheme. *IEEE Access* **2019**, *7*, 118943–118953. [CrossRef]
21. Tanwar, S.; Parekh, K.; Evans, R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *J. Inf. Secur. Appl.* **2020**, *50*, 102407. [CrossRef]
22. Du, M.; Chen, Q.; Chen, J.; Ma, X. An optimized consortium blockchain for medical information sharing. *IEEE Trans. Eng. Manag.* **2020**, *68*, 1677–1689. [CrossRef]
23. Liu, J.; Jiang, W.; Sun, R.; Bashir, A.K.; Alshehri, M.D.; Hua, Q.; Yu, K. Conditional Anonymous Remote Healthcare Data Sharing Over Blockchain. *IEEE J. Biomed. Health Inform.* **2023**, *27*, 2231–2242. [CrossRef] [PubMed]

24. Tandon, A.; Dhir, A.; Islam, A.N.; Mäntymäki, M. Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. *Comput. Ind.* **2020**, *122*, 103290. [CrossRef]
25. Xi, P.; Zhang, X.; Wang, L.; Liu, W.; Peng, S. A review of Blockchain-based secure sharing of healthcare data. *Appl. Sci.* **2022**, *12*, 7912. [CrossRef]
26. Eluubek kyzy, I.; Song, H.; Vajdi, A.; Wang, Y.; Zhou, J. Blockchain for consortium: A practical paradigm in agricultural supply chain system. *Expert Syst. Appl.* **2021**, *184*, 115425. [CrossRef]
27. Triulzi, I.; Antonel, A.; Rossi, E.; Turchetti, G. Public Hospital Supply Chain: Current View And Critical Issues In Italy. *Value Health* **2017**, *20*, A515–A516. [CrossRef]
28. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017.
29. Sagirlar, G.; Carminati, B.; Ferrari, E.; Sheehan, J.D.; Ragnoli, E. Hybrid-iot: Hybrid blockchain architecture for internet of things-pow sub-blockchains. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1007–1016.
30. Nyaletey, E.; Parizi, R.M.; Zhang, Q.; Choo, K.K.R. BlockIPFS-blockchain-enabled interplanetary file system for forensic and trusted data traceability. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 18–25.
31. Muralidharan, S.; Ko, H. An InterPlanetary file system (IPFS) based IoT framework. In Proceedings of the 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 11–13 January 2019; pp. 1–2.
32. Batchu, S.; Henry, O.S.; Hakim, A.A. A novel decentralized model for storing and sharing neuroimaging data using ethereum blockchain and the interplanetary file system. *Int. J. Inf. Technol.* **2021**, *13*, 2145–2151. [CrossRef]
33. Dunphy, P.; Petitcolas, F.A. A first look at identity management schemes on the blockchain. *IEEE Secur. Priv.* **2018**, *16*, 20–29. [CrossRef]
34. Ateniese, G.; Fu, K.; Green, M.; Hohenberger, S. Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage. *ACM Trans. Inf. Syst. Secur. (TISSEC)* **2006**, *9*, 1–30. [CrossRef]
35. Liang, K.; Au, M.H.; Liu, J.K.; Susilo, W.; Wong, D.S.; Yang, G.; Yu, Y.; Yang, A. A secure and efficient Ciphertext-Policy Attribute-Based Proxy Re-Encryption for cloud data sharing. *Future Gener. Comput. Syst.* **2015**, *52*, 95–108. [CrossRef]
36. Shabtai, A.; Menahem, E.; Elovici, Y. F-Sign: Automatic, Function-Based Signature Generation for Malware. *Trans. Syst. Man Cybern. Part C* **2011**, *41*, 494–508. [CrossRef]
37. Wang, Y.; Ding, Y.; Wu, Q.; Wei, Y.; Qin, B.; Wang, H. Privacy-Preserving Cloud-Based Road Condition Monitoring With Source Authentication in VANETs. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 1779–1790. [CrossRef]
38. Zeng, P.; Choo, K.K.R. A New Kind of Conditional Proxy Re-Encryption for Secure Cloud Storage. *IEEE Access* **2018**, *6*, 70017–70024. [CrossRef]
39. Ge, C.; Liu, Z.; Xia, J.; Fang, L. Revocable identity-based broadcast proxy re-encryption for data sharing in clouds. *IEEE Trans. Dependable Secur. Comput.* **2019**, *18*, 1214–1226. [CrossRef]
40. Agyekum, K.O.B.O.; Xia, Q.; Sifah, E.B.; Cobblah, C.N.A.; Xia, H.; Gao, J. A proxy re-encryption approach to secure data sharing in the internet of things based on blockchain. *IEEE Syst. J.* **2021**, *16*, 1685–1696. [CrossRef]
41. Zheng, X.; Zhou, Y.; Ye, Y.; Li, F. A cloud data deduplication scheme based on certificateless proxy re-encryption. *J. Syst. Archit.* **2020**, *102*, 101666. [CrossRef]