Hindawi
Security and Communication Networks
Volume 2021, Article ID 5523489, 10 pages
https://doi.org/10.1155/2021/5523489

Research Article

Controlled Sharing Mechanism of Data Based on the Consortium Blockchain

Jin Li,[1] Songqi Wu,[1] Yundan Yang,[1] Fenghui Duan,[1] Hui Lu,[2] and Yueming Lu[1]

[1]*School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2]*Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou 510006, China*

Correspondence should be addressed to Hui Lu; luhui@gzhu.edu.cn

Received 19 January 2021; Revised 18 February 2021; Accepted 8 March 2021; Published 22 March 2021

Academic Editor: Qi Li

In the process of sharing data, the costless replication of electric energy data leads to the problem of uncontrolled data and the difficulty of third-party access verification. This paper proposes a controlled sharing mechanism of data based on the consortium blockchain. The data flow range is controlled by the data isolation mechanism between channels provided by the consortium blockchain by constructing a data storage consortium chain to achieve trusted data storage, combining attribute-based encryption to complete data access control and meet the demands for granular data accessibility control and secure sharing; the data flow transfer ledger is built to record the original data life cycle management and effectively record the data transfer process of each data controller. Taking the application scenario of electric energy data sharing as an example, the scheme is designed and simulated on the Linux system and Hyperledger Fabric. Experimental results have verified that the mechanism can effectively control the scope of access to electrical energy data and realize the control of the data by the data owner.

1. Introduction

Regarding the threat of data leakage, Verizon summarized the 2019 Data Breach Investigation Report (DBIR) to provide important points. In response to real data on 41,686 security incidents and 2013 data breaches from a total of 73 data sources from 86 countries, DBIR noted that the median direct loss to the threatened organization was $8,000 for a commercial e-mail threat and $25,000 for a computer data breach. Among them, there were 927 data leakage incidents in the financial and insurance industries. Network application attacks, abuse of privileges, and various errors accounted for 72%. It can be seen from this that data leakage losses from all walks of life are huge. In the process of storing and sharing data, there are mainly risks of data tampering and data leakage [1–4] due to single points of failure in centralised storage centres, malicious tampering, and inadequate access control mechanisms, so it is vital to find a way to achieve trusted storage and controlled flow of data.

Blockchain [5], as the core technology of recording the transaction book history of bitcoin system, has been widely concerned by all sectors of society since its inception. With the gradual development of Ethereum and Hyperledger Fabric, its features such as distributed storage and smart contract deployment and enforcement provide new ideas for solving data leakage problems in data sharing.

By taking advantage of the decentralized storage and data nontampering [6, 7] and data traceability features of blockchain, it is possible to achieve trusted storage of data and avoid the risks of centralised data storage such as single point of failure and data tampering.

The existing main methods of data protection using blockchain technology focus on the realization of secure data storage scheme [8]. However, after uploading the data to the blockchain, it is also crucial to ensure that the shared data can be trusted by controlling the boundaries of the data flow and achieving controlled data sharing. In traditional blockchain networks, all nodes are explicitly visible to the data on the chain, which does not apply to some sharing scenarios like electric energy data sharing. Therefore, blockchain data being visible to all user nodes can be a disadvantage in the realization. To address the

problem of data leakage due to explicit storage of data [9], consortium blockchain Hyperledger Fabric provides multichannel [10] data isolation protection method, so that the data is only visible to the joint maintenance account book of each organization and node in the channel, which enables effective control over the extent of data flows. However, there is still a risk of leakage after the nodes in the channel access the data on the chain during the sharing of data; at the same time, it does not meet the need for granular and complex access control of the data in the chain.

Therefore, in combination with attribute-based cryptography [11], it is possible to formulate data access policies for user-specific access and decryption. The data provider can formulate a data access policy based on the identities and attributes of the users to complete the granular access control of the data. Simultaneously, the data access process is recorded in the private account ledger that cannot be tampered by the data owner, so as to guarantee the traceability of data lifecycle processes. This paper proposes a mechanism that can realize trusted storage of data and granular access control and lifecycle management process for recording of data and take electric energy data sharing as an example to realize controlled sharing of electric energy data. The specific contributions of this paper are as follows:

(1) This paper presents a trusted storage scheme for electrical energy metadata by constructing electrical energy data storage consortium blockchain. Through the description of standardized metadata on the chain and the combination of distributed file system FastDFS, the chain aggregation storage of electric energy private data is realized, which solves the problems of high timing requirement and large amount of data in the storage of electric energy privacy data and provides the technical basis for controllable sharing and safe utilization of electric energy data.

(2) Using attribute-based encryption technology, based on the existing Fabric-CA in Hyperledger Fabric, implement user attributes key dynamic generation and safe distribution operations, which solve the problems of key abuse and privacy data leakage due to the ability of private key generator to decrypt all data in traditional attribute-based encryption technology. It realizes the data owner to formulate a data access policy based on the identities and attributes of the users to complete the granular access control of the data. It also effectively solves the key distribution challenges associated with traditional ABE encryption schemes.

(3) Using the privacy data mechanism proposed by Hyperledger Fabric [12], the data owner records the data access process to form a private ledger that can be seen only by the access data participants, which is used as the maintenance ledger of their own data to ensure the traceability of the controlled data flow process.

The related work and background are introduced in the second section. The third section shows the controlled sharing mechanism of electrical energy data based on consortium blockchain. The fourth section presents the experimental results and analysis. The fifth section provides a summary of the paper and puts forward the direction of future work.

2. Related Work and Background

For the study of trusted storage and access control of electrical energy data based on blockchain, a cloud blockchain fusion model (CBFM) is proposed in [13]. The power data is accurately identified through the image of parallel vision system in the cloud, and the power data storage scheme based on blockchain is implemented by using Hyperledger Fabric, which solves the problem of safe and accurate storage of electric energy data, but it does not consider the problems of data leakage in the process of storage and sharing of a large amount of electric energy data. A blockchain-based multiparty computing scheme is proposed in [14], and solutions are proposed for the fairness issues in MPC, as well as a solution for the secure sharing of data [15]. An SGX-based approach to blockchain for IoT applications is presented. Multiple Intel Software Guard Extensions (SGX) distributed Oracle servers are utilized to ensure data availability, combined with Intel SGX and TLS communication to ensure data integrity. In [16], a blockchain block authentication scheme based on group signatures is proposed. The solution is proposed to address the problem of limited computing resources of mobile blockchain devices. It also ensures the traceability of transaction data and distributed deployment of computational resources.

In [17], a trusted data acquisition model for power systems is proposed in conjunction with blockchain technology. The model realizes the authenticity of the underlying equipment state parameters of the power grid. In order to protect the privacy information in the power consumption data, a blockchain-based privacy data and identity protection scheme is proposed in [18]. The group membership data is recorded in a private blockchain, and, by using pseudonyms, the user's private identity within the group is hidden, and fast authentication of identity is achieved in combination with a Bloom filter. To address the issue of data privacy and leakage in IoT systems, a blockchain-based IoT architecture [19] has been proposed, which enables data access control, privacy, and confidentiality of data shared in a blockchain-based IoT ecosystem. It uses the attribute encryption (ABE) technique to ensure authenticity and ensure the privacy and confidentiality of shared data in the IOT [20, 21]ecosystem based on blockchain.

Reference [22] proposes a framework for storage sharing based on blockchain, IPFs, and ABE. Complete policy control of data access by the owner by distributing keys for blockchain transactions realizes data encryption sharing and granular access control in distributed storage Ethereum system.

It can be seen from the above research that, combined with the storage structure of distributed file system and attribute-based encryption algorithm, the trusted storage and controlled sharing mechanism of electric energy data can be realized by building the consortium blockchain, which can be used as a continuous framework for the interaction of electric energy data calculation and storage, so as to meet the application requirements of large-scale electric energy data trusted sharing in the future.

2.1. Blockchain and Hyperledger. Bitcoin, as the earliest technical application of blockchain technology, has attracted widespread attention because of its decentralized, unalterable, and traceable transaction characteristics. From a data perspective, blockchain technology is essentially a distributed database that collectively maintains and stores all historical transaction data in a decentralized and trustless way. The distributed ledger maintained by blockchain only supports query and addition but does not support modification and deletion. The use of hash linked list and Merkel tree structure ensures that no node can illegally tamper with the ledger.

Hyperledger Fabric [23, 24] is the representative of enterprise-level open-source blockchain. It has proposed many schemes in terms of permission control and privacy protection, in which version 1.2 has started to support the application of privacy Transaction (SideDB). The privacy transaction protection method caches the temporary database through the authorized endorser, synchronizes the transaction to other authorized endorsers and committers through the gossip protocol, and finally returns the hash value of the key-value pair of the private data to the client node to complete the endorsement. In the client phase, the client phase submits the hashes of the privacy data to the sorting service node for the normal winding-up process. After the block containing the transaction is synchronized to the whole network nodes, the authorized node checks and synchronizes the privacy data according to the authorization policy and then verifies the integrity of the privacy data according to the hash value of the public transaction. Finally, in the process of ledger submission, the authorized node updates from the temporary cache database to the private ledger to realize the recording and protection of privacy data.

Fabric CA is the digital certificate authentication center of Hyperledger, which mainly provides the functions of user identity registration, digital certificate issuance, and digital certificate extension and revocation. Before adding transaction information to Hyperledger Fabric, it is necessary to obtain legal identity authentication from authentication authorization node (CA peer) and then package the transaction information into blocks for broadcast throughout the network. All nodes in the network can verify the legitimacy and effectiveness of the transaction. Finally, the consensus mechanism is used to realize the consensus of all nodes in the network, and legal blocks are joined in the blockchain so that the information on transactions cannot be tampered with.

2.2. FastDFS Distributed File System. FastDFS [25] is an open-source lightweight distributed file system developed by Using C language, which can work well on UNIX-like systems and pursue high performance and high scalability. The overall design is based on the principle of simplicity and efficiency to solve the problem of large user access and large capacity file storage. FastDFS has good performance of redundant backup, load balancing, and online expansion, which is suitable for storing small-sized and medium-sized files, such as documents, pictures, and multimedia files.

FastDFS distributed file system is mainly composed of tracker, storage, and client [26]. Tracker is mainly responsible for the scheduling of storage, and multiple tracker clusters are formed in pairs to achieve load balancing. Storage is mainly responsible for file storage and redundant backup. FastDFS uses grouping mechanism to divide storage cluster into GROUPs and realizes load balancing, application isolation, and copy number customization independently among groups [27]. There can be multiple storage servers in the same group. The storage in the group is also peer-to-peer. The storages in the same group are connected with each other for file synchronization. The storage capacity of a group is subject to the storage with the smallest memory storage capacity of the group. When the system capacity is insufficient, the horizontal expansion can be realized by adding the group. When the storage access pressure in a group is too large, the vertical expansion can be realized by adding storage in the group. The client side of FastDFS is an application server using FastDFS access interface, which can be deployed on it by using its own development projects.

2.3. Attribute-Based Encryption Technology. Goyal et al. were the first to propose attributed-based encryption, which uses identity to define a series of attribute sets, and its definition is divided into key policy attribute-based encryption (KP-ABE) and ciphertext policy attribute-based encryption (CP-ABE) [28]. The CP-ABE is related to the secret message, the user's private key, and the set of attributes. The user can only decrypt the plaintext message for access control if the generated private key and the set of attributes embedded in the secret message match, and the access control policy matches exactly. Simultaneously, the granularity of the ciphertext accessibility control mechanism can be flexibly selected according to the strictness of the specified policy when the encryption or key is generated. In the application scenario of electric energy data sharing, the data owner determines the access user list of encrypted data, and the CP-ABE associated with decryption strategy and ciphertext can better meet the data demand of electric energy sharing and realize the access control of data on the chain.

3. System Model

The controlled sharing mechanism of data based on the consortium blockchain is mainly composed of the data storage consortium blockchain construction method, the distributed file system FastDFS application, and the distributed application DAPP (Decentralized Application) program development.

The construction of the data storage consortium blockchain ensures that the underlying data storage cannot be modified and uses attribute-based encryption to complete data access control to meet the needs of granular access control and secure sharing of data. Through the construction of a data flow transfer book, the original data life cycle management is recorded, and each data control is effectively recorded. Party's data transfer process. The distributed file system FastDFS solves the storage expansion problem of the data storage consortium blockchain and, based on its lightweight and developable nature, realizes the return of the source data ciphertext storage path and the source data file hash calculation operation, and the file hash is on the chain data storage data description providing a basis to authenticate the data integrity; the storage paths are used for recording in the current ledger records and the data providers can control the life cycle of data by changing the storage location. Distributed application (DAPP) is a decentralized operation application running on the blockchain network, which can better store user information and protect user privacy. In the controlled sharing mechanism of electric energy data based on the consortium blockchain, distribution through deployment of the distributed application DAPP realizes client operations such as data on-chain storage, controlled access, and data lifecycle management. This article takes the meter code table record storage and controlled access scenario in the electric energy metering system as an example to effectively solve the problem of safe storage and controlled sharing of electric energy data. The overall scheme is shown in Figure 1.

The electric energy data storage consortium chain utilizes the Hyperledger Fabric architecture at the bottom and uses the smart contract to realize the controlled access to the chain of electric energy data based on attribute-based encryption and the data life cycle management based on the fabric private data, so as to realize the safe storage, controlled access, and life cycle management of the electric energy data. On the distributed file system FastDFS, the return of the secret storage path of the source data of electric energy and the hash calculation of the source data file are realized, and the returned hash value is stored in the blockchain as the description of the data file, and, through the calculated hash value of the file, the electric energy data integrity verification function can be realized; the secret storage path of the source data of electric energy and the decryption key of the source data secret are used to access the transaction to form a private transaction. Recorded in the data owner's private ledger, the distributed application DAPP is used to realize client operations such as the storage of electric energy data on the chain and the completion of electric energy data access transactions. The specific construction process is as follows.

3.1. Construction of Electric Energy Data Storage Consortium Blockchain. The structure of the power energy data storage union chain is shown in Figure 2. The system is composed of a variety of intelligent terminal devices, each collection master system, blockchain system, FastDFS distributed file system, and distributed application (DAPP) integrated client. After the electric energy data is generated by intelligent terminal equipment, it is transmitted to the main station of acquisition system through wireless transmission network or optical fiber network. The main station of the system is composed of data center and control center.

The control center realizes client visualization by building DAPP. The data center realizes distributed storage by using FastDFS. The control center encrypts the source data to the data center through DAPP and transmits the file hash and data description and source data returned by FastDFS to the consortium blockchain network through Fabric-SDK-Go interface. The consortium blockchain calls smart contracts to aggregate and process the electric energy data to form metadata. After the data is standardized, the data is encrypted with attributes and is then uploaded. The nodes of the consortium blockchain run a consensus algorithm together and enter the data into the electrical energy data store through audit checks. The consortium blockchain forms a ledger structure to realize the decentralized safe and reliable storage and access control of electric energy data. Each data owner and access node initiate data access request and reply through smart contract and form access transaction records in the participant's private ledger to realize the data owner's life cycle management of data.

3.2. Electric Energy Data Access Control Policy. CP-ABE is used to implement an access control solution for electrical energy data storage consortium blockchain sharing. With the help of Fabric-CA module, CP-ABE initialization, key generation, and distribution operations are realized, and electric energy data encryption and chain operation are completed by using smart contract. The attribute definition of CP-ABE is realized by using channel ID, organization ID, and user ID in Hyperledger network as user attributes, and the access control policy is defined by the data provider to achieve access control of the data in the blockchain. The specific operation process is mainly divided into three stages: key generation and distribution, data encryption chain, and access control.

In the phase of key generation and distribution, the initialization and key generation and distribution are mainly completed by Fabric-CA and DAPP through Fabric-SDK-Go communication. By inputting the system security parameter λ, the main public key PK and key MK in CP-ABE scheme are generated:

$$\text{Setup}\left(1^{\lambda}\right) \longrightarrow (\text{MK}, \text{PK}). \tag{1}$$

The UCR is the certificate request submitted by the user, and Fabric-CA generates the user key SK related to the attribute set A for the user requestor using a randomization code based on the attribute set A in the user request and uses the user public key U_{PK} in UCR to encrypt the user key SK to form ciphertext CT_{usk} and attach the certificate U_{cert} issued by Fabric-CA for the user. Simultaneous interpreting cert. is sent to the user requester.

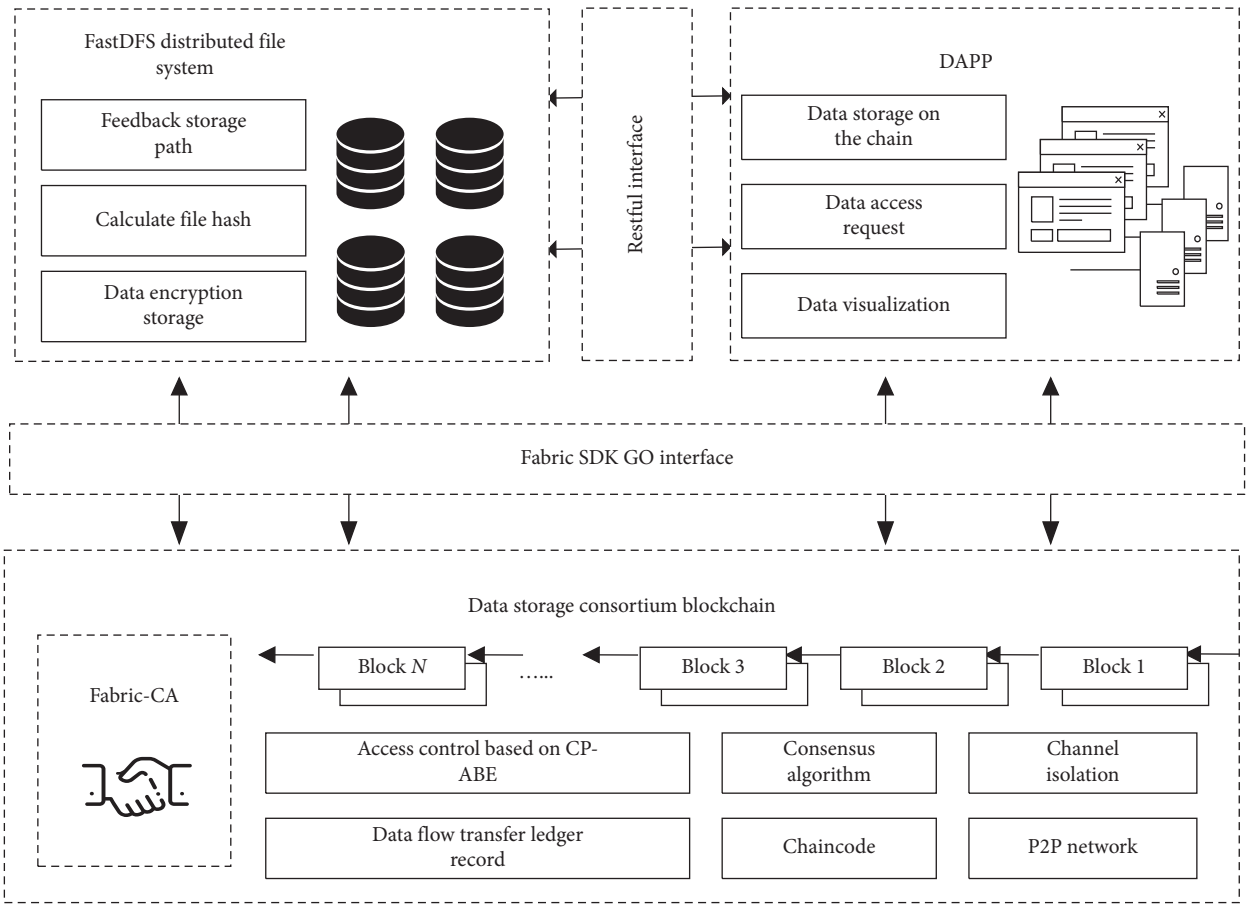

Figure 1: The overall scheme of controlled sharing mechanism of data based on the consortium blockchain.

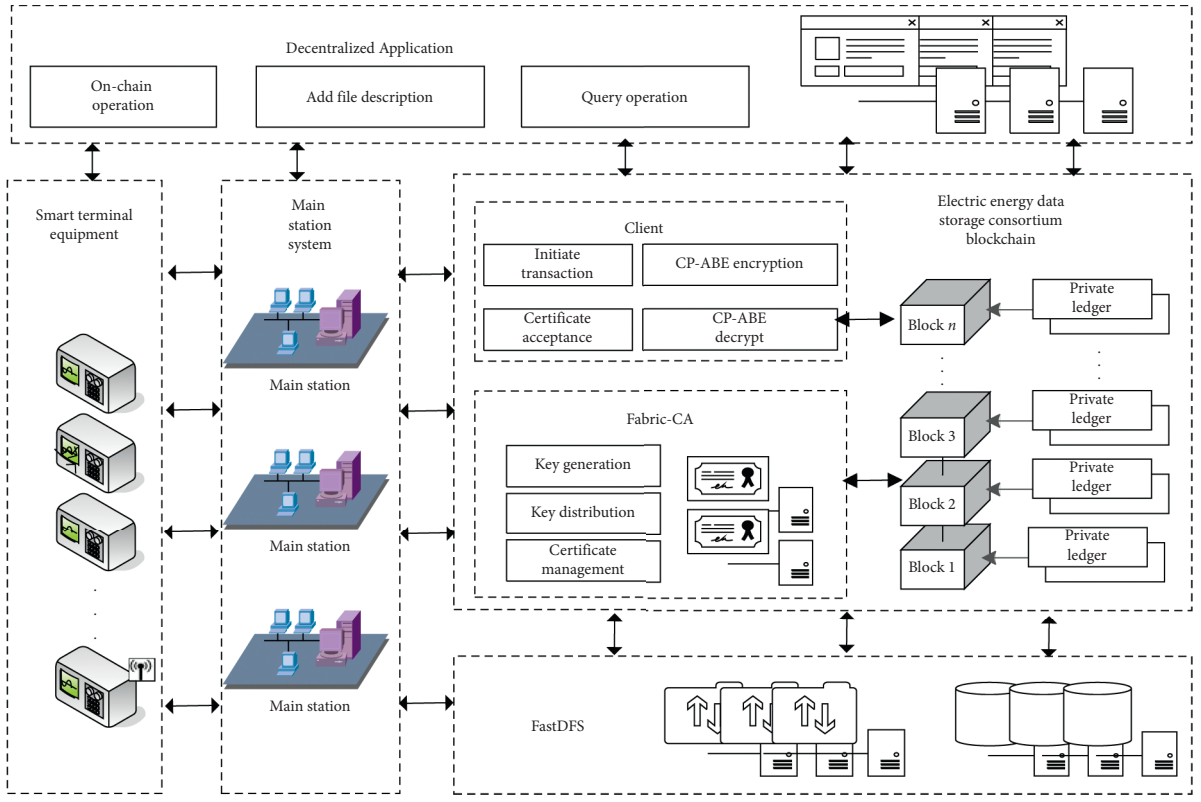

Figure 2: Electric energy data storage consortium blockchain structure.

$$\text{KeyGen}(\text{PK}, \text{MK}, A) \longrightarrow \text{USK}. \quad (2)$$

In the data encryption stage, before submitting the link-up request, the data owner uses the randomization algorithm to encrypt the submitted data in an attribute-based manner. The algorithm is input into the system public key PK and the data to be encrypted T_A and access control policy P_A generate ciphertext CT_A based on attribute encryption.

$$\text{Encrypt}(\text{PK}, T_A, P_A) \longrightarrow \text{CT}_A. \quad (3)$$

In the access control stage, after the data owner links the encrypted data to the chain, other users request the corresponding information of the transaction ciphertext in the blockchain network through the client to obtain the corresponding ciphertext CT_A. Decrypt the ciphertext by using the visitor attribute key USK. When the private key attribute meets the policy P_A in CT_A, the user can decrypt to get the plaintext M_A corresponding to the encrypted data, andimplement user level access control.

$$\text{Decrypt}(\text{CT}_A, \text{PK}, \text{USK}) \longrightarrow T_A. \quad (4)$$

3.3. Construction of Electric Energy Data Life Cycle Management Ledger. SideDB based on Hyperledger realizes the life cycle management of data for the data owners in the power energy data consortium blockchain. The transaction ledger is formed by recording the access process of the original data of the electric energy data, which is maintained in the private ledger of the data access participants.

The hash values of private transactions are also publicly recorded on the chain to enable verification of transactions. The data owner can complete the life cycle management and access control of the data by changing the source data storage path and data encryption key. The specific process of forming the ledger is shown in Figure 3.

Data visitors submit data access requests to data owners through DAPP. Data owners sign messages and verify their identities. For example, DAPP submits access transactions including data access party, data storage path, and data decryption key in FastDFS. Temporary database is cached by authorized endorser. Gossip protocol realizes message synchronous access transaction to other authorized endorsers and committers. Then, the hash value of the key-value pair of the access transaction data is returned to the data owner client node to complete the endorsement. The data providing client stage submits the hash value of the access transaction data to the ordering service node for normal uplink process. After the block containing the access transaction is synchronized to the whole network node, the transaction participant node checks and synchronizes the privacy data according to the authorization policy and then verifies the integrity of the privacy data according to the hash value of the public transaction. Finally, in the process of ledger submission, the transaction participant node updates from the temporary cache database to the private ledger to realize the access record of electric energy data and the control of the data owner on the original data.

Its smart contract design is shown in Algorithm 1. The user sends a transaction request to the accounting node and submits his own attribute set Role = $(r_1, r_2, \ldots, r_n)$, and the accounting node verifies according to the requested file KeyId and the search area and the blockchain ledger verifies whether the user complies with the access control policy of shared files. If the user matches, the accounting node will check whether it owns the metadata of the file and, if so, send the subkey to the requesting user. The user can decrypt the ciphertext to obtain the metadata set and download the file according to the metadata set. The data holder records the transaction behavior and records the user, file storage address, and attribute key in a personal privacy database.

4. Performance Analysis

A prototype experiment is designed to analyze the performance and feasibility of the solution. The experimental environment is configured with an Intel Core i5 processor, 16 GB of RAM, 460 GB of hard disk space, an Ubuntu 16.04LTS desktop, and programming languages Java and Go. The blockchain is deployed by Hyperledger Fabric. Three servers with official Fabric clients are deployed as blockchain nodes and smart contracts are deployed. According to the definition of access control policy for CP-ABE, three basic attributes are selected: channel ID, organization ID, and user ID. The three peers belong to the same channel CHANEL1 and two organizations Org1 and Org2, and the user IDs are CHANEL1. Org1. User1, CHANEL1. Org1. User2, and CHANEL1. Org2. User1. The access control policies are defined randomly.

The experimental data are recorded in the code table of China Southern Power Grid Co, Ltd. from 2014 to 2015, and the minimum data unit is about 120,000 15 MB data generated at the same time node. In order to verify the authenticity and effectiveness of the controlled sharing mechanism of electric energy data, three key links in the controlled sharing mechanism are selected for testing. The three key links are as follows: the system encrypts and stores the electric energy data to FastDFS, uploads the electric energy data description to the blockchain, and forms the account book of the electric energy data access transaction. We test the time consumption of each link.

4.1. Performance Test of Electric Energy Data Storage to FastDFS. In order to realize the reliable sharing of electric energy data, the power grid system is divided into different subregions in the production scenario, and the power consumption situation of the area is reported regularly. FastDFS is used to upload the hourly electric energy data and extract the file size, storage location, and other information as the description of electric energy data.

In the experiment, 15.0 MB files generated by 12,000 collection nodes were selected as the minimum granularity of upload data. The number of uploaded files was increased from 1 to 50, and the impact on the performance of data uploading to FastDFS distributed file system module was tested. The experimental results are shown in Figure 4, and

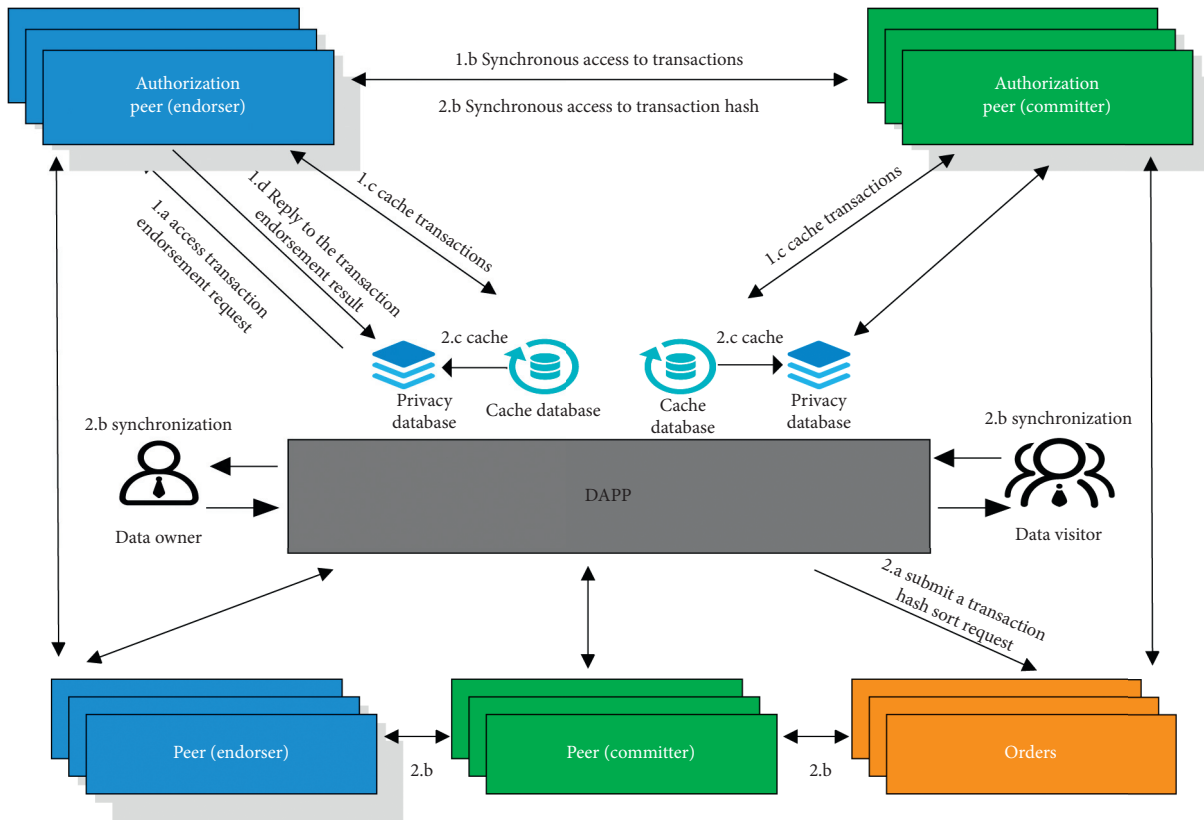

Figure 3: The process of forming the ledger.

Input: User, KeyID, node
Output: bool
(1) send Request To Node (KeyId, Role), ←User
(2) retrieve Ledger (KeyId)
(3) getAcp (KeyId)
(4) foreach $i \in$ Role
(5) **if** verifyRole (i) == ture **then**
(6) **break**
(7) **else**
(8) refuse
(9) flag = searchLocalDatabase (KeyId)←node
(10) **if** flag == ture **then**
(11) response (key_{share}) ⟶ User
(12) address = getPiter←User
(13) download (address)←User
(14) decrypt (key_{share})
(15) (User, uri, key_{share}) ⟶ SideDB
(16) **return** true;

Algorithm 1: Algorithm of data access transaction.

the upload time of electric energy data files to FastDFS increased from 213 ms to 12049 ms, the hash time increased from 42 ms to 3363 ms, and the total time increased from 255 ms to 15412 ms.

As the number of file uploads increases, the FastDFS upload storage and file hash calculation time increases linearly, and the time consumption of uploading data to FastDFS storage is relatively large.

4.2. Performance Test of Electric Energy Data Description Encryption Chain. The client node releases the electric energy data and uploads it to the blockchain request. The blockchain node requests to call the chain code and input the hash of the electric energy data file and other data descriptions as parameters, executes the chain code to realize CP-ABE encryption, and writes the execution result of the chain code into the blockchain ledger after

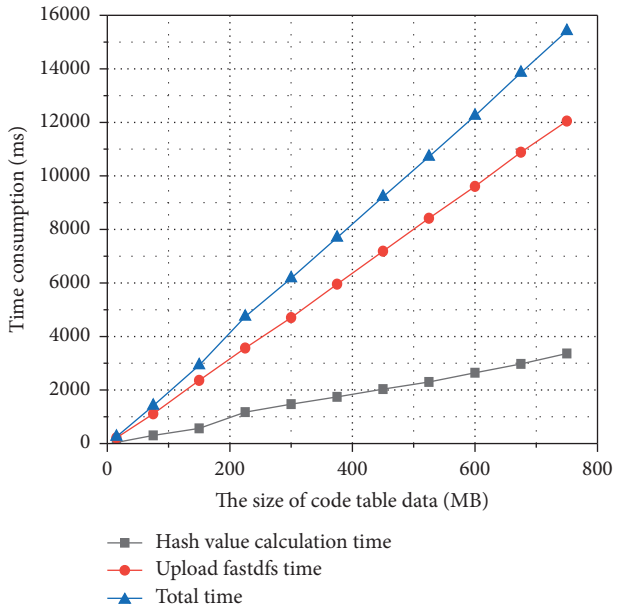

Figure 4: The experimental results of electric energy data storage to FastDFS.

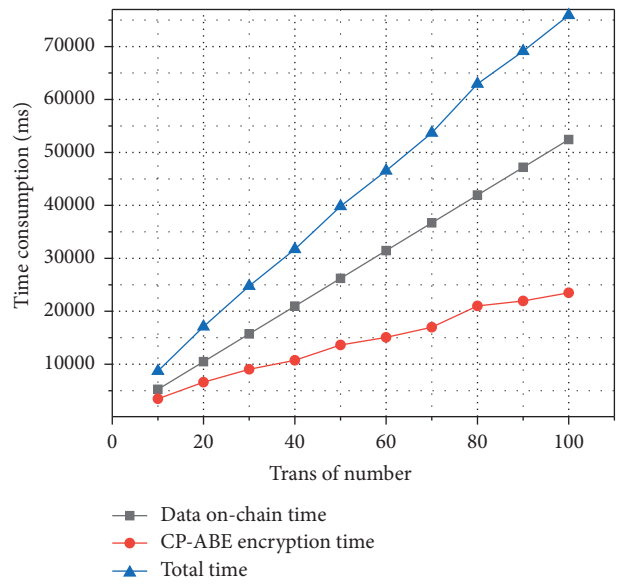

Figure 5: The experimental results of electric energy data description encryption chain.

reaching a consensus among the nodes. The experimental results are shown in Figure 5.

Assuming that 10~100 electric energy data records are added to the blockchain ore pool in the same period of time, the time for test encryption and chain connection to reach a consensus is about 8.72 s–75.916 s. The data encryption time is 3.47s~23.48 s, and the data link time is 5.25 s~52.43 ms. The reason is that DAPP is based on Fabric-SDK-Go platform. It needs docker-compose to generate fabric image, instantiates chain code to interact with fabric platform, and uses restful interface to call chain code to realize opening up, which is different from fabric throughput concept.

4.3. Performance Test of Electric Energy Data Access Transaction Ledger. The transaction ledger is formed by recording the access process of the original data of electric energy data, which is maintained in the privacy ledger of the data access participants.

The experiment measures the transaction delay and compares the access transaction query with the public transaction query. The results are shown in Figure 6. In a period of time, 10~100 access transactions are uploaded to form the access transaction account book, and the average time for reaching a consensus is initially 421 ms. As the network environment becomes stable, the average time consumption decreases to 361.61 ms. The average time consumption of public transaction query and access transaction query tends to be stable, with the average of 283.55 ms and 218.24 ms. It can be seen that the query efficiency of access transaction ledger stored in private ledger is lower than that of public transaction query, but it is within the acceptable range of users.

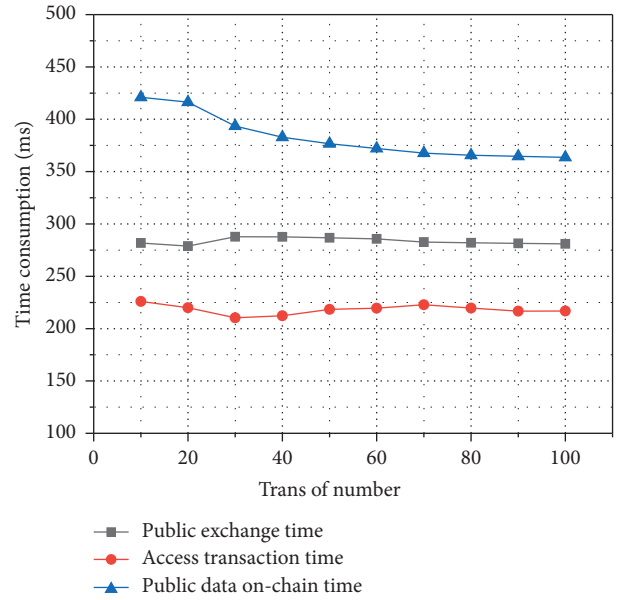

Figure 6: The experimental results of electric energy data access transaction ledger.

5. Conclusion and Future Work

This paper proposes a data-controlled sharing framework, which provides a new solution for data secure storage and controlled sharing. Realize the credible storage of data by building a data storage consortium blockchain, using ABE to complete data access control, meeting the need for granular access control and secure sharing of data, and controlling the scope of data flow; by building a data flow transfer book to record original data life cycle management, the data transfer process of each data controller is effectively recorded, so that the data owner can complete the life cycle management and

access control of the data by changing the source data storage path and data encryption key.

In the future, we will address the security issues facing the secure sharing of data and applications between blockchains. In this paper, although we propose a data-controlled sharing framework, it will be useful to maintain data sharing between multiple blockchains to meet data sharing scenarios.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

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

Acknowledgments

This work was supported by the National Key R&D Program of China (Grant no. 2019YFB2102400).

References

[1] M. Li, Y. Sun, H. Lu, S. Maharjan, and Z. Tian, "Deep reinforcement learning for partially observable data poisoning attack in crowdsensing systems," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6266–6278, 2020.

[2] Z. Tian, C. Luo, J. Qiu, X. Du, and M. Guizani, "A distributed deep learning system for web attack detection on edge devices," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1963–1971, 2020.

[3] Q. Tan, Y. Gao, J. Shi, X. Wang, B. Fang, and Z. Tian, "Toward a Comprehensive Insight Into the Eclipse Attacks of Tor Hidden Services," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1584–1593, 2019.

[4] H. Lu, C. Jin, X. Helu et al., "Research on intelligent detection of command level stack pollution for binary program analysis," *Mobile Network and Applications*, 2020.

[5] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[6] C. Xu, K. Wang, P. Li et al., "Making big data open in edges: a resource-efficient blockchain-based approach," *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 4, pp. 870–882, 2019.

[7] P. Danzi, A. E. Kalor, C. Stefanovic, and P. Popovski, "Analysis of the communication traffic for blockchain synchronization of IoT devices," in *Proceedings of the 2018 IEEE International Conference on Communications (ICC)*, pp. 1–7, Kansas City, MO, USA, May 2018.

[8] H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu, and J. Xing, "Hyperconnected network: a decentralized trusted computing and networking paradigm," *IEEE Network*, vol. 32, no. 1, pp. 112–117, 2018.

[9] H. Lu, C. Jin, X. Helu, C. Zhu, N. Guizani, and Z. Tian, "AutoD: intelligent blockchain application unpacking based on JNI layer deception call," *IEEE Network*, vol. 99, pp. 1–7, 2020.

[10] *A Blockchain Platform for the Enterprise—Hyperledger-Fabricdocs Master Documentation*, https://hyperledger-fabric.readthedocs.io/en/release-1.3/.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS 2006)*, pp. 89–98, Alexandria, VA, USA, October 2006.

[12] E. Androulaki, A. Barger, V. Bortnikov et al., "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth EuroSys Conference (EuroSys '18)*, pp. 1–15Article 30, New York, NY, USA, April 2018.

[13] S. Cao, J. Zou, X. Du, and X. Zhang, "A successive framework: enabling accurate identification and secure storage for data in smart grid," in *Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC) IEEE*, pp. 1–6, Dublin, Ireland, June 2020.

[14] H. Gao, Z. Ma, S. Luo, and Z. Wang, "BFR-MPC: a blockchain-based fair and robust multi-party computation scheme," *IEEE Access*, vol. 7, pp. 110439–110450, 2019.

[15] S. Woo, J. Song, and S. Park, "A distributed oracle using intel SGX for blockchain-based iot applications," *Sensors*, vol. 20, no. 9, p. 2725, 2020.

[16] S. Zhang and J. H. Lee, "A group signature and authentication scheme for blockchain-based mobile-edge computing," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4557–4565, 2019.

[17] T. Yang, F. Zhai, J. Liu, M. Wang, and H. Pen, "Self-organized cyber physical power system blockchain architecture and protocol," *International Journal of Distributed Sensor Networks*, vol. 14, no. 10, 2018.

[18] Z. Guan, G. Si, X. Zhang et al., "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 82–88, 2018.

[19] Y. Rahulamathavan, C. W. Phan, S. Misra, and M. Rajarajan, "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption," in *Proceedings of the 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp. 1–6, Bhubaneswar, India, December 2017.

[20] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "CorrAUC: a malicious Bot-IoT traffic detection method in IoT network using machine learning techniques," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3242–3254, 2020.

[21] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, "A survey on access control in the age of Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4682–4696, 2020.

[22] W. Shangping, Z. Yinglong, and Z. Yaling, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, vol. 6, pp. 38437–38450, 2018.

[23] S. Nathan, P. Thakkar, and B. Vishwanathan, "Performance benchmarking and optimizing hyperledger fabric blockchain platform," in *Proceedings of the 2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, pp. 264–276, Milwaukee, WI, USA, September 2018.

[24] J. Sousa, A. Bessani, and M. Vukolic, "A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform," in *Proceedings of the 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 51–58, Luxembourg City, Luxembourg, June 2018.

[25] H. Che and H. Zhang, "Exploiting FastDFS client-based small file merging," in *Proceedings of the International Conference on Artificial Intelligence & Engineering Applications*, pp. 242–246, Hong Kong, China, November 2016.

[26] X. Liu, Q. Yu, and J. Liao, "FastDFS: a high performance distributed file system," *ICIC Express Letters. Part B, Applications: An International Journal of Research and Surveys*, vol. 5, no. 6, pp. 1741–1746, 2014.

[27] M. R. Kaseb, M. H. Khafagy, I. A. Ali, and E. S. M. Saad, "Redundant independent files (RIF): a technique for reducing storage and resources in big data replication," in *Trends and Advances in Information Systems and Technologies*, pp. 182-183, Springer, Berlin, Germany, 2018.

[28] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the IEEE Symposium on Security & Privacy*, pp. 321–334, Berkeley, CA, USA, May 2017.