STAIBT: Blockchain and CP-ABE Empowered Secure and Trusted Agricultural IoT Blockchain Terminal

Guofeng Zhang[1]*, Xiao Chen[2], Lei Zhang[3], Bin Feng[1]*, Xuchao Guo[4], Jingyun Liang[5], Yanan Zhang[6]

[1] School of Information Science and Technology, Taishan University, Taian Shandong (China)
[2] School of Economics and Management, Taishan University, Taian Shandong (China)
[3] Shandong Academy of Macroeconomic Research, Jinan Shandong (China)
[4] College of Information and Electrical Engineering, China Agricultural University, Beijing (China)
[5] Laboratory of Quality and Safety Risk Assessment for Agro-Products of the Ministry of Agriculture (Jinan), Institute of Quality Standard and Testing Technology for Agro-Products, Shandong Academy of Agricultural Sciences, Jinan Shandong (China)
[6] School of Information Science and Engineering, University of Jinan, Jinan Shandong (China)

Received 14 December 2021 | Accepted 25 April 2022 | Published 28 July 2022

Abstract

The integration of agricultural Internet of Things (IoT) and blockchain has become the key technology of precision agriculture. How to protect data privacy and security from data source is one of the difficult issues in agricultural IoT research. This work integrates cryptography, blockchain and Interplanetary File System(IPFS) technologies, and proposes a general IoT blockchain terminal system architecture, which strongly supports the integration of the IoT and blockchain technology. This research innovatively designed a fine-grained and flexible terminal data access control scheme based on the ciphertext-policy attribute-based encryption(CP-ABE) algorithm. Based on CP-ABE and DES algorithms, a hybrid data encryption scheme is designed to realize 1-to-N encrypted data sharing. A "horizontal + vertical" IoT data segmentation scheme under blockchain technology is proposed to realize the classified release of different types of data on the blockchain. The experimental results show that the design scheme can ensure data access control security, privacy data confidentiality, and data high-availability security. This solution significantly reduces the complexity of key management, can realize efficient sharing of encrypted data, flexibly set access control strategies, and has the ability to store large data files in the agricultural IoT.

Keywords

Agricultural Internet Of Things, Blockchain, Ciphertext-Policy Attribute-Based Encryption(CP-ABE), Data Security, Privacy Protection.

DOI: 10.9781/ijimai.2022.07.004

I. Introduction

As the key technology of agricultural informatization, agricultural IoT has made enough and outstanding achievements all over the world. Nevertheless, the traditional agricultural IoT that uses a centralized storage architecture is facing problems such as data privacy leakage, data tampering, data untrusted and so on. The decentralization, non-tampering and traceability of blockchain provide new technologies and new ideas for the development of agricultural informatization and IoT, making it rapidly become an important technology in many applications of precision agriculture [1].

On the whole, the integrated application of blockchain and IoT technology has become a new research hotspot in the field of agricultural information. As a distributed ledger, each node of blockchain stores complete ledger data. How to ensure the security and privacy of the data stored in the ledger is a topic that cannot be bypassed by the research and application of blockchain technology. Unauthorized access to IoT devices can cause serious privacy and security issues, and has become a major challenge hindering the widespread adoption of IoT technology [2]. Agricultural IoT terminal is an important source of agricultural data, and its privacy protection and access control are very important for the data security management of the whole life cycle of Agricultural IoT. How to protect the privacy and security of agricultural data from the data source is the starting point and goal of this research.

This work is dedicated to the technical integration of blockchain and IoT. Through the introduction of cryptography technology, we design a data encryption and access control scheme suitable for IoT terminals, and finally design a secure and trusted agricultural IoT blockchain terminal. The main contributions of this paper are as follows:

1. A system architecture of a universal IoT blockchain terminal based on cryptography, blockchain and IPFS technology is proposed. It inherits the advantages of the traditional Internet of Things terminal, and at the same time has the technical characteristics of directly acting as a blockchain and IPFS node. Make it an effective carrier for the integrated application of blockchain and the Internet of Things.

* Corresponding author.
E-mail addresses: binfeng@tsu.edu.cn (Bin Feng), zhangguofeng@tsu.edu.cn (Guofeng Zhang).

2. Based on the ciphertext-policy attribute-based encryption(CP-ABE) algorithm, a fine-grained and flexible terminal data access control scheme is designed. The innovative use of the IoT terminal as an effective means of data access control realizes the binding of data access control and data collection equipment. At the same time, the experimental results show that the scheme will not affect the storage efficiency of blockchain data.
3. A hybrid data encryption scheme is designed. With the help of the fine-grained access control scheme designed in this paper, it can not only realize 1-to-N encrypted data sharing, but also significantly reduce the complexity of key management.
4. A "horizontal + vertical" segmentation plan for IoT data is proposed.Combining the hybrid data encryption scheme and IPFS storage proposed in this paper, it realizes the efficient storage, security and trusted fine-grained authorized access of IoT data.

The following organizational structure of this paper is: Section II summarizes the related works of this work; section III briefly introduces the two key technologies used in this paper; section IV designs and proposes the architecture, data access control, data segmentation and privacy protection schemes of the secure and trusted agricultural Internet of Things data terminal, and further introduces the algorithm designed in this paper; section V describes the experiment. According to the experimental results, the advantages of this design scheme are systematically analyzed from two aspects of security and performance; section VI gives the conclusion of this paper.

II. Related Works

A. Blockchain and Agricultural IoT

Recent studies have conducted a comprehensive investigation on the blockchain and the IoT in precision agriculture, and proposed a new blockchain model [1]. The security of equipment in precision agriculture is a key issue of the IoT, and the integration of blockchain and IoT technology can provide a new solution to this problem [2]. The agricultural IoT is more vulnerable to attacks than other industrial scenarios. Based on the blockchain and IoT technology, a new identity verification and key management scheme is designed, called AKMS-AgriIoT [3], in which encryption and verification are made by the General Satellite Service (GSS) is completed and submitted to the blockchain system. The use of limited-function sensing devices in the IoT as a reliable data source for the blockchain has been studied, and it is believed that the integration of blockchain and IoT can be applied to the agricultural production process [4]. In the process of pre production and post production of agriculture, through the integration of blockchain, smart contracts and IoT devices, trust has been established between all parties and a fully automated process has been completed [5]. The traditional fish farm system and the Hyperledger Fabric blockchain can perform Integration [6], the device client uses embedded hardware such as Raspberry Pi and Arduino to communicate with the traditional fish farm system and the blockchain. As a super node [7], Raspberry Pi 3B can safely process and aggregate field data and push it to the blockchain ledger. In precision agriculture applications, it is believed that every IoT node can interact with the ledger and directly record data on the ledger [7]. In the agricultural supply chain system, the Fabric with IPFS is used. It can effectively promote the construction of quality traceability system of agricultural products supply chain [8]. The design of agricultural product supply chain scheme based on blockchain should ensure that data encryption storage is safe and reliable, the transaction records can be traced, queried and appealed, and private data is owned by each participant [9].

It can be seen that blockchain and agricultural IoT have been widely studied from theory to technology. However, the above research in agricultural IoT focuses on the integration of the two, and there is no clear scheme for data sharing, access control and privacy protection in blockchain. In particular, how to realize data privacy protection and access control on the device side of the IoT is the starting point and goal of this paper.

B. Blockchain Data Sharing and Access Control

Hyperledger blockchain is dedicated to providing brand new solutions for data security and privacy protection [10],[11]. A Secure and Reliable Traceability System for Agricultural Products Powered by Permissioned BlockChain Technology is proposed, and the fine-grained authorized access and agricultural product quality and safety traceability mechanism under the CP-ABE algorithm is discussed [12]. HyperLedger fabric has been used in the pharmaceutical traceability system [13]. Jemel et al. [14] and Huang Sui et al. [15] discussed data sharing methods based on blockchain and CP-ABE technology. Wang Xiuli et al. [16] proposed data access control and sharing model using ABE for fine-grained access control and secure sharing. Based on ABAC and blockchain, Zhang et al. [17] use access trees to configure access policies to enable fine-grained authorized access to IoT devices. However, the IoT devices need to use the blockchain proxy node to interact with the blockchain ledger, and there is a risk of data being tampered with at the collection end.

C. Block Data Encryption and Privacy Protection

Data confidentiality is a prerequisite for ensuring data security. The security of block (ledger) data is mainly guaranteed by encrypting transaction data with encryption algorithm, and its access rights should also be considered. CP-ABE algorithm has been used in blockchain system to realize flexible data authorization access [18]. To support more flexible public key generation, Sahai and Waters [19] first proposed an Attribute-based Encryption (ABE) scheme, which uses a set of attributes rather than a unique identifier to identify the identity. ABE is a kind of fine-grained 1-to-N encryption scheme.

Further research has proposed the key-policy Attribute-based Encryption (KP-ABE) [20] and the ciphertext-policy Attribute-based Encryption (CP-ABE) [21]. KP-ABE embeds the policy into the encryption key and the attributes into the ciphertext. CP-ABE embeds the policy into the ciphertext and the attributes into the user key. The common feature of both is that the encryption and decryption of data are bound to the access policy, and only when the attributes in the attribute set can satisfy the access structure can the data be decrypted . Fine-grained access control can be achieved while retaining cryptographic control. However, the application scenarios of the two are different. The KP-ABE scheme stores the encrypted ciphertext on the server.It assigns a specific access policy to the user when access is granted, commonly used for paid video sites, log encryption management,etc. In the CP-ABE scheme, as long as it has corresponding attributes and satisfies its logical relationship, ciphertext data can be automatically decrypted, which is more suitable for one-time encryption and multiple authorized private data sharing, such as encrypted data sharing in cloud storage.

Symmetric encryption system has the characteristics of fast speed and shared keys between encryption and decryption parties. Although it can also be used for blockchain data encryption, with the increasing complexity of business transactions between organizations and the dynamic change of the number of organizations, key distribution and management will become more and more complex. Moreover, there will be problems such as key leakage and multiple encryption.

In view of the above analysis, this article uses the CP-ABE algorithm and the symmetric encryption DES algorithm to design a hybrid encryption scheme suitable for IoT terminals. It can encrypt sensitive data collected by IoT terminals and perform flexible access control on

data on the chain. While ensuring data security, the complexity of key management is further reduced.

III. Preliminaries

A. CP-ABE

The data in the blockchain ledger is shared to the all nodes of blockchain, and is easily accessed illegally. The CP-ABE scheme sets access control policies based on data attributes and is used for data encryption. Anyone who has the attributes in the access control policy and satisfies the logical relationship can decrypt the data. Because it doesn't care about specific users at all, it has more flexibility in access control. Therefore, this paper introduces the CP-ABE algorithm to guarantee data confidentiality and authorized access control of the data sharer. It realizes the unification of ownership and control of data in blockchain.

The CP-ABE encryption algorithm [21] composed of five basic algorithms, including Setup, Encrypt, KeyGen, Decrypt and Delegate. Among them, CT = Encrypt (PK, M, T) is the encryption algorithm, which can encrypt the plaintext message M under the public key PK and the access control tree T into ciphertext CT, the specific as in (1).

$$CT = (T, \check{C}, C, \forall y \epsilon Y: C_y, C'_y) \tag{1}$$

$$\check{C} = Me(g,g)^{as} \tag{2}$$

$$C = h^s \tag{3}$$

$$C_y = g^{q_{y(0)}} \tag{4}$$

$$C'_y = H(att(y))^{q_{y(0)}} \tag{5}$$

Here, the parameters α, s are random, and g is the generator of the bilinear group of prime order. Let G1 and G2 be two multiplicative cyclic groups of prime order p,g be a generator of G1 and e be a bilinear map e : G1 × G1 ⟶ G2.

The parameters y is the leaf node of access structure T,q_y is a polynomial for each node y in the tree T . The ciphertext CT is constructed by T, which is the tree access structure. The function att(x) is defined only when x is a leaf node and represents the attribute associated with the leaf node x in T.

The decryption function is DecryptNode (CT, SK, x), defined as in (6).

$$DecryptNode(CT, SK, x) = \frac{e(D_i, C_x)}{e(D'_i, C'_x)} = \frac{e(g^r \cdot H(i)^{r_i}, h^{q_x(0)})}{e(g^{r_i}, H(i)^{q_x(0)})} \tag{6}$$

$$DecryptNode(CT, SK, x) = e(g,g)^{r q_x(0)} \tag{7}$$

Here, SK is a private, which is associated with a set of S attributes, and a node x from T.

For the explanation of other parameters, refer to the literature [21]. However, the above two formulas and the parameters T and attr(x) show that attributes are the essential for data encryption and decryption and access control in the CP-ABE algorithm. It determines the flexibility of the access control policy and who can decrypt the ciphertext data.

B. IPFS

InterPlanetary File System (IPFS) is a point-to-point distributed file system, a network transmission protocol designed by Juan Benet and open source management by Protocol Labs, which can provide permanent and distributed storage of files. Integrating the technical advantages of P2P, Git, BitTorrent, Kademlia, Self-certifying File System (SFS) and Web, it can provide a simple interface similar to HTTP Web. Its distributed storage technology can be perfectly matched with blockchain technology to boost the ability of the blockchain system to store large files. For example, IPFS integrated with blockchain technology for agricultural products supply chain traceability system [22].

IV. The Proposed Schemes and Algorithms

A. System Architecture of a IoT Blockchain Terminal

This paper is focused on the protection of agricultural IoT data security and access control. With the empowerment of blockchain and cryptography technology, a universal secure and trusted agricultural IoT blockchain terminal is designed. Its architecture is shown in Fig. 1.

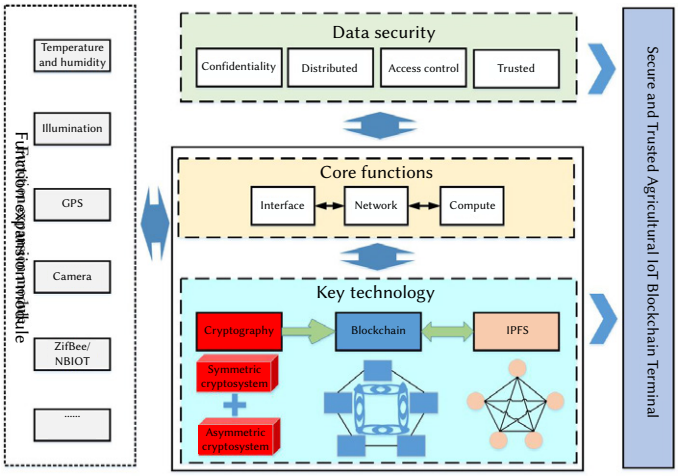


Fig. 1. General secure and trusted agricultural IoT blockchain terminal architecture.

This architecture is still based on traditional embedded technology and has a wealth of functional expansion interfaces to facilitate the access of sensors and expansion modules. From a functional and technical point of view, this system uses blockchain and IPFS technology to realize distributed storage of collected data. With the help of symmetric encryption and asymmetric encryption mechanisms, it can protect data privacy, set flexible access control, and finally provide secure and trusted IoT data collection service. Its typical feature is that the terminal integrates blockchain, IPFS, cryptography and embedded systems, and can be used as a gateway to the agricultural IoT, providing raw data directly on the chain at the collection end, protecting data security from the source.

Deploying the blockchain and IPFS system directly in the terminal system puts forward certain requirements for embedded hardware and software. The data segmentation and encryption algorithm designed in this paper belongs to a part of the terminal embedded software. It interacts with blockchain and IPFS to realize the uplink release of encrypted data. As an ARM-based microcomputer motherboard, the Raspberry Pi has almost all the basic functions of a PC, making it one of the best choices for the integration of IoT terminals and blockchain. This paper will also be based on the Raspberry Pi 4B development board for experimental verification. In view of the limited storage capacity of the embedded system, the terminal device may not store the complete blockchain ledger data, but is only used to publish the data.

B. Terminal Data Access Control Scheme

1. Terminal Registration

This paper regards the IoT terminal as an access control object. First, the terminal must be registered and connected to the network. The administrator sets the private data encryption key, terminal number,

attributes and related parameters for the terminal. These parameters constitute a unique file for the device to collect. Data access control is called an access control file.

2. Fine-Grained Access Control Algorithm

The core function of Agricultural IoT system is to automatically perceive and obtain the process data of the three stages before, during and after agricultural production. This work is mainly completed automatically by the IoT terminal, and the continuous data presents typical dynamic and serialization characteristics. All the collected data include the serial number, name and other key information of the IoT terminal. Obviously, the access control of IoT data can also be transformed into the access control of IoT terminals. In this paper, the serial number and other key information of the IoT terminal and the key of data encryption are written into a unique file to set a flexible and fine-grained access control policy for the terminal. Therefore, this file is named device access control file. The access control policy of the file can be expressed in the form of access tree, as shown in Fig. 2.

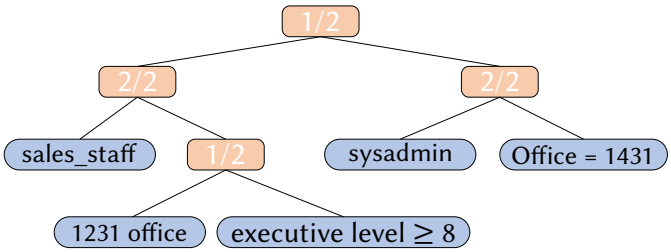


Fig. 2. Access tree model.

Fig. 2 shows an access control tree model. This is an example of setting access control policies on the basis of employee attributes. The logical meaning of the access control tree is as follows.

1. Employees with sysadmin attribute in 1431 office.
2. Sales staff with execution level greater than or equal to 8, in 1231 office.

This paper realizes one-time encryption and n-time sharing of data. When the access user has the attributes in the access tree and can meet its logical relationship, the secret data can be decrypted correctly.

3. Access Control Smart Contract

We create an access control file for each terminal, which contains the key and access control policy used by the terminal for data encryption. To protect the data privacy of the file and to perform flexible access control, encryption is performed using the CP-ABE algorithm. However, please note that the CP-ABE ciphertext of this file will take up more storage space than the plaintext. The specific amount occupied is related to the number of data attributes used for encryption. Obviously, this is not conducive to the on-chain storage of the file. Therefore, this paper uses IPFS for file storage, meanwhile, publishes the hash value in IPFS through the authorized access control smart contract. The name of the designed access control smart contract is auth, which includes the design of the access control structure and the related operation functions of access control.

```
// AuthSet describes authset details of what makes up a simple
   authset
 type AuthSet struct {
    ID          string      'json:"ID"'
    Terminal    string      'json:"terminal"'
    Authinfo    string      'json:"authinfo"'
}
```

According to the above analysis, the access control file of each device corresponds to the access control data, including the Terminal number and the access control authentication information Authinfo. In the follow-up experiments of this paper, in order to facilitate the experiment, Authinfo is mainly used to store the key information encrypted by the device, which will be introduced in section V.B.

C. Privacy Data Segmentation and Encryption Scheme

1. Data Segmentation

The secure and trusted agricultural IoT blockchain terminal can collect different data in agricultural production scenarios, such as data such as temperature, humidity, and light in agricultural greenhouses, fields, and other production environments, as well as video, voice, and image data. To ensure the performance of the blockchain system, data segmentation technology is adopted to segment the above data, and a " horizontal + vertical " IoT data segmentation scheme is designed. Specifically:

First, the horizontal data segmentation. The IoT data is divided into structured data and unstructured data. Generally speaking, structured data is relatively standardized, occupies less storage space, and can be stored on the blockchain normally. Unstructured data occupies more storage space. Therefore, it needs to be stored with the help of IPFS file system, which can not be affected by file size.

Secondly, vertical data segmentation. Separate private data and public data in structured data. Separate the sensitive and private data on the blockchain and perform encryption processing to better ensure data privacy.

Through the data segmentation technology, the classified storage of structured data and unstructured data, and the classified processing of sensitive data and public data are realized, making the data collected by safe and trusted terminals more standardized and clear.

2. Privacy Data Encryption

The symmetric encryption system has the advantage of fast speed. Under the premise of ensuring the security of the key, it can fully meet the confidentiality requirements of the data on the blockchain. This paper uses the DES symmetric encryption algorithm to encrypt the private data on the blockchain and the unstructured private data stored in IPFS. As the key for the symmetric encryption algorithm, the key is stored in the access control policy file. Only users with access rights to the device can decrypt the key, thereby ensuring the security of private data.

Therefore, a hybrid encryption scheme is constructed by CP-ABE and DES algorithms, combined with data segmentation technology, which can protect data confidentiality and achieve fine-grained authorized access to data. Among them, the data segmentation and privacy data encryption scheme process is shown in Fig. 3.

3. Data Publish Smart Contract

The data collected by a secure and trusted IoT blockchain terminal needs to be published on the blockchain with the help of a blockchain smart contract. The data publish smart contract defines the structure of the data set. At the same time, it defines operation functions such as the initialization of the ledger, the creation of data sets, and the query.

```
type DataSet struct {
    ID          string      'json:"ID"'
    Terminal    string      'json:"terminal"'
    User        string      'json:"user"'
    Airtemp     float32     'json:"airtemp"'
    Airhumi     int         'json:"airhumi"'
    Illu        int         'json:"illu"'
    Gps         string      'json:"gps"'
}
```

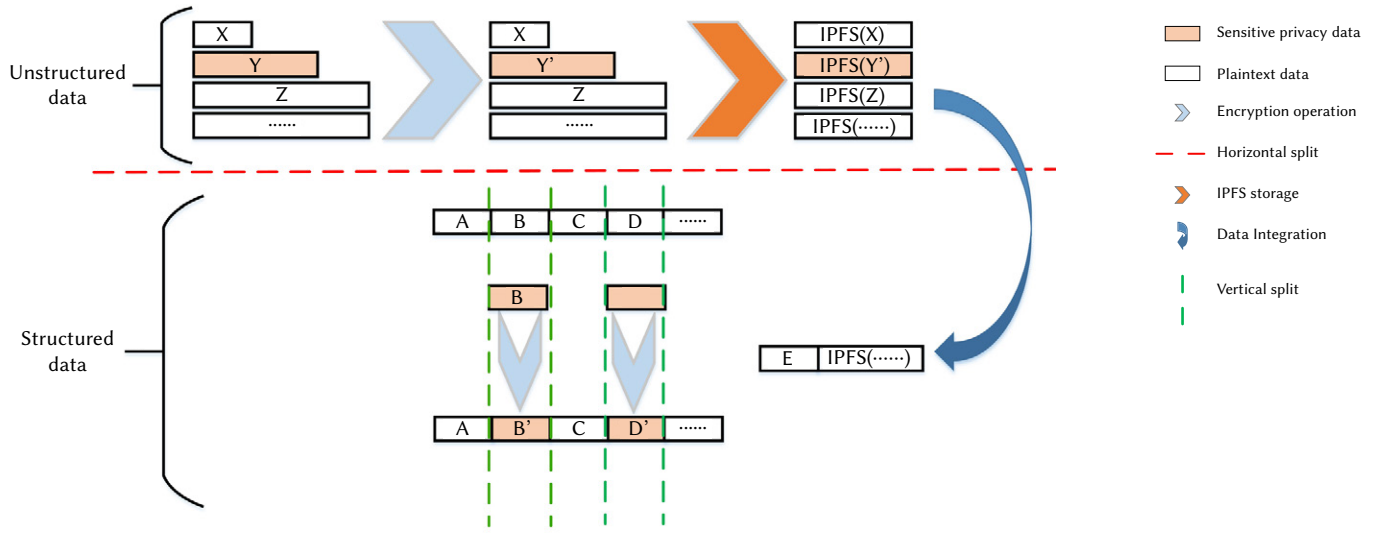


Fig. 3. The data segmentation and privacy data encryption scheme process.

This paper takes the greenhouse environment data of the agricultural IoT system as an example, and designs a data set DataSet, where ID is used to represent the data number, Terminal represents the number of the terminal, User represents the user number, Airtemp represents the air temperature, and Airhumi represents the air humidity, Illu means light intensity, Gps means the current coordinates of the device. In section V, this smart contract will be experimentally verified.

4. Proposed Algorithm

According to the above design scheme, this work designs the terminal security registration algorithm, block data access control algorithm and secure trusted data encryption uplink algorithm. Algorithm 1 and algorithm 2 show the pseudo codes of the latter two algorithms respectively.

The terminal security registration algorithm is to construct an access control policy, which determines the flexibility and accuracy of data sharing. The symbolic variables are shown in Table I.

Algorithm 1: Block data access control algorithm
Input: Block data retrieval conditions, user private key
Output: Query result data of the ledger
begin:
  BlockData = ChaincodeQuery (sect, retrieval conditions);
  if (Does it contain ciphertext data?)
    AuData= ChaincodeQuery(auth,Terminal number);
    ct_acfile =IPFS_Get(AuData.authinfo);
    acfile=Cpabe-dec(ct_acfile,user private key);
  if (Has the decryption succeeded?)
    DES_Decrypt (BlockData.ciphertext, acfile.TelKey);
    return the complete data after decryption;
  else
    return BlockData containing ciphertext;
  else
  return BlockData;
end

Algorithm 2: Secure trusted data encryption uplink algorithm
Input: Data collected by Agriculture IoT terminals, Encryption key
Output: Secure and trusted blockdata under privacy protection
begin:
  StData, UstData=HorizontalDatasplit(Data);
  SensitiveCheck(StData,UstData);
  if (Is unstructured data?)
    if (Is sensitive data?)
      Ciphertext = DES_Encryption(UstData.StData);
      UstFile = CreateCiphertext_file(Ciphertext);
    else
      UstFile = CreateCiphertext_file(UstData);
    H(UstFile) = IPFS_add(UstFile);
    upData = DataMerge(Terminal number,H(UstFile));
    ChainCodeInvoke = (sect,upData);
  else
    PData, SData = VerticalDataSplit(StData);
    While (Is sensitive data encrypted?) do
      Ciphertext[] = DES_Encryption(SData);
  upData = DataMerge(PData, Ciphertext[]);
  ChainCodeInvoke = (sect,upData);
end

TABLE I. Symbolic Variables

Variable name	Meaning
Tid	Terminal identifier or number
A	Attributes set
TK	Terminal data encryption key
Acf	Access control file
Acf'	Ciphertext of access control file
H	The identification of the ciphertext of the access control file in IPFS
D	Terminal attributes and data
UD	Data that needs to be stored on the chain
S	Terminal security registration smart contract

$$CreatAC\_File(Tid, A, TK) \rightarrow Acf \tag{8}$$

The *CreateAC_File* function generates an access control policy based on attributes, and generates an access control file based on terminal parameters.

$$Cpabe\_enc(Acf, TK) \rightarrow Acf' \tag{9}$$

The *Cpabe_enc* function performs CP-ABE encryption on the access control file.

$$IPFS\_add(Acf') \rightarrow H \tag{10}$$

The *IPFS_add* function uploads the ciphertext access control file to the IPFS system and receives the hash value of the file H, that is, the unique identification of the file.

$$DataMerge(Tid, D, H) \rightarrow UD \tag{11}$$

The DataMerge integrates the terminal number and the file's hash into the chaindata.

$$ChainCodeInvoke(UD, S) \tag{12}$$

Finally, auth chaincode is called to publish the chaindata on the blockchain.

In Algorithm 1, when there is a ciphertext in the blockdata that the user queries, and it is determined that the ciphertext needs to be decrypted, it will go to the IPFS to retrieve the access control file of the terminal. The IPFS file downloaded by the IPFS_Get function needs to be decrypted by Cpabe_dec. Only when the current user attribute (private key) meets the access control strategies can the decryption succeed. After the decryption is successful, the DES algorithm key for encrypting the terminal data is obtained.The key cannot be decrypted without access control privileges, thereby protecting the user's data privacy.

The core of Algorithm 2 is data segmentation. HorizontalDatasplit divides data into structured and unstructured data, and VerticalDataSplit divides structured data into public data and sensitive data. Then perform data encryption and data integration depended on the split results and the sensitivity of the data, and finally publish it on the blockchain. The classification and hierarchical processing of data are realized to ensure the privacy and security of data.

V. Experiments

In this section, we simulate the experimental results and analyze of the proposed scheme.

A. Materials and Environment

The hardware experiment environment in this paper includes secure and trusted terminal nodes and PC nodes. The safe and trusted terminal node uses the Raspberry Pi Pi 4B development board, 8GB of memory, 64GB of storage, integrated temperature and humidity sensor DHT11, GPS module, and light sensor BH1750FVI, as shown in Fig. 4.

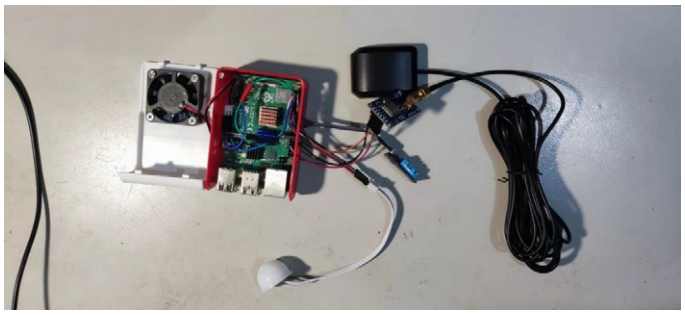


Fig. 4. Secure and trusted agricultural IoT blockchain terminal.

The software system of the terminal is: x64 Ubuntu Server 20.04 LTS operating system, HyperLedger Fabric 2.1.0 blockchain platform, and the node data collection and encryption and decryption programs are developed in C language. The open source CP-ABE algorithm is used in the experiment [23]. In order to test the access control and data encryption designed in this paper, a blockchain network including 1 Orderer node and 2 Peer nodes was built in the Raspberry Pi system, as shown in Fig. 5. Among them, Peer nodes belong to organization 1 and organization 2, and the development of smart contracts adopts the Golang language.

```
fabric@ubuntu:~/go/fabric-samples/test-network$ docker ps -a
CONTAINER ID   IMAGE                         COMMAND               CREATED          STATUS         PORTS                                            NAMES
9f51e686f748   busan15/fabric-peer:latest    "peer node start"     13 seconds ago   Up 9 seconds   7051/tcp, 0.0.0.0:9051->9051/tcp, :::9051->9051/tcp   peer0.org2.example.com
ba8cab62f206   busan15/fabric-orderer:latest "orderer"             13 seconds ago   Up 9 seconds   0.0.0.0:7050->7050/tcp, :::7050->7050/tcp        orderer.example.com
74f16467c561   busan15/fabric-peer:latest    "peer node start"     13 seconds ago   Up 9 seconds   0.0.0.0:7051->7051/tcp, :::7051->7051/tcp        peer0.org1.example.com
fabric@ubuntu:~/go/fabric-samples/test-network$
```

Fig. 5. Blockchain network process.

B. Data Access Control Policy Experiment

1. Data Access Control Policy Encryption

In this experiment, there are three employees in the IoT data center, administrators Sara and LeBron, sales staff Kevin, and the system assigns private keys to them based on key attributes such as their identities and positions. Specifically, Sara and LeBron both have sysadmin attributes, but Sara is in the office of 1431 and LeBron is in the 1531 office. Kevin has the sales_staff attribute, has an employee level of 7, and is in the 1231 office.

The number of the secure and trusted blockchain terminal in the experiment is T0000001, and its key of private data encryption is 123456, the name of the designed data access control policy file is T0000001.txt, and the content is "Congratulations. The key of T00000001 is 123456". According to Fig. 2 in Section IV.B, set a data access control policy for it, and perform CP-ABE encryption. Therefore, the encryption command is:

cpabe_enc pub_key T0000001.txt (sysadmin and office=1431) or (sales_staff and (executive_level ≥ 8or office = 1231))

After encryption, the T0000001.txt.cpabe file will be created. The content is the ciphertext of T0000001.txt, as well as the attributes and access control policies that can correctly decrypt the file, so as to ensure the confidentiality of the data and flexible access control.

2. Access Control File Operation

The IPFS file system generates a unique hash value while storing the data access control file T0000001.txt.cpabe, as shown in Fig. 6. This hash value is called and the access control smart contract auth is published on the blockchain, thereby realizing the access control file on the blockchain. The data visitor can retrieve the hash value of the access control file with terminal number T0000001 in IPFS by calling the smart contract, as shown in Fig. 7, obtain the file locally through the IPFS interface or command, and then rename it to the terminal number, as shown in Fig. 8.

Fig. 9 shows the process of access control policy verification. For LeBron, even though he has sysadmin attributes, he is not in the 1431 office, so he cannot decrypt the access control file to get the key, and he cannot obtain the private data collected by the terminal, but can only see the non-sensitive data. On the contrary, although Kevin's level is not enough, he is in the 1231 office and has the sales_staff attribute, so he can correctly decrypt the access control file and obtain the encryption key of the terminal T0000001 from the file content as 123456. There is no doubt that Sara can also decrypt the key.

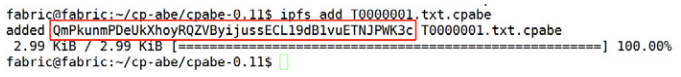


Fig. 6. Access control file upload to IPFS system.

Fig. 7. Publish access control files on the blockchain.

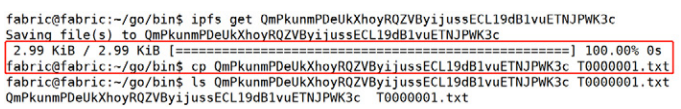


Fig. 8. Download the access control file from the IPFS system.

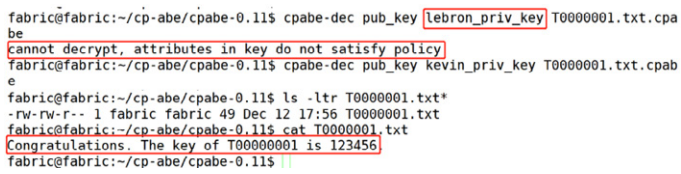


Fig. 9. Access control policy verification.

The experimental results have shown that the scheme designed can realize the fine-grained authorized access of data encryption keys, thereby realizing one-time encryption and multiple sharing, and reducing the complexity of key management.

C. Private Data Encryption Experiment

In this experiment, the trusted terminal can collect the five parameters of air temperature, air humidity, light intensity, and GPS, and publish it on the blockchain together with the terminal number T000001 and user information Test0001. In order to protect the privacy of the data owner, the data on the chain can be sliced into sensitive data and public data. Among them, sensitive data is encrypted using encryption algorithms, and the ciphertext is published, so as to realize data desensitization and protect user privacy.

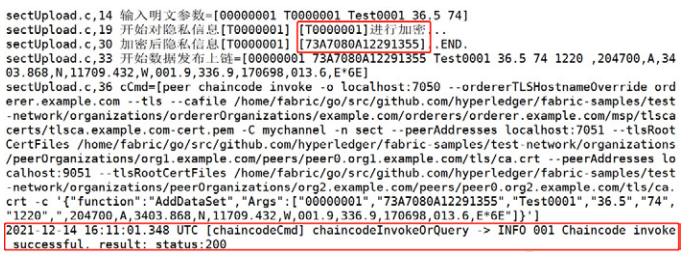


Fig. 10. Publish private data encryption on the blockchain.

Fig. 10 shows the above-mentioned data segmentation, data encryption, and publishing process. In the experiment, the user ID T00000001 in the data is divided into sensitive data by using the data segmentation technology. It is encrypted by DES encryption algorithm with key 123456, and the ciphertext 73a708a12291355 is calculated. By calling the AddDataSet function in the sect smart contract, the sensitive data and public data are published on the blockchain together, and the response code "200" indicates that the data publish is successful.

D. Encrypted Data Storage Space Experiment

The CP-ABE encryption operation will cause the ciphertext data to occupy more storage space. In order to verify the influence of CP-ABE encryption operation on the storage space of ciphertext data, three experiments are designed in this section. details as follows:

Experiment 1. Perform CP-ABE encryption on plaintext data with file sizes of 49b, 98b, 147b, and 196b. The encryption attributes and access control policy is "(sysadmin and office=1431) or (sales_staff and (executive_level ≥ 8 or office = 1231))". The storage space occupied by ciphertext and plaintext is shown in Table II.

TABLE II. Experiment 1 Storage Space Occupation Results

Plaintext size (bit)	Increment size (bit)	Cipher-text (bit)	Increment (bit)	Additional (bit)
49	-	3066	-	3017
98	49	3114	48	3016
147	49	3162	48	3015
196	49	3162	48	3014

Experiment 2. Perform CP-ABE encryption on plaintext data with file sizes of 49b, 98b, 147b, and 196b. The encryption attributes and access control policy is "(sysadmin and office=1431)". The storage space occupied by ciphertext and plaintext is shown in Table III.

TABLE III. Experiment 2 Storage Space Occupation Results

Plaintext size (bit)	Increment size (bit)	Cipher-text (bit)	Increment (bit)	Additional (bit)
49	-	921	-	872
98	49	969	48	871
147	49	3162	48	3015
196	49	3162	48	3014

Experiment 3. Perform CP-ABE encryption on "libmultipath.so.0" files with a file size of 384848b, respectively, using encryption attributes and access control policy A, namely "(sysadmin and office=1431) or (sales_staff and (executive_level ≥ 8 or office = 1231))" and B, namely "(sysadmin and office=1431)". The storage space occupied by ciphertext and plaintext is shown in Table IV.

TABLE IV. Experiment 3 Storage Space Occupation Results

Plaintext size (bit)	Access control policy	Cipher-text (bit)	Additional (bit)
384848	A	387866	3018
384848	B	385721	873

The results of Experiment 1 show that with the same encryption attributes and access control policy, the space occupied by the ciphertext is positively correlated with the space occupied by the plaintext. For example, when the plaintext space increases by 49, the ciphertext space increases by 48 in response. The results of Experiment 1 and Experiment 2 jointly show that for the same plaintext data, the space occupied by the ciphertext is positively related to the encryption attributes and access control policies adopted. For example, the data of 49b adopts two different access control policies, which occupy 3018b, 872b of storage space.

More importantly, the additional ciphertext storage space caused by encryption attributes and access control policies is fixed. The results of Experiment 3 proved the above point, such as encryption attributes and access control policy A will increase the storage of 3018b, and B

will increase the storage of 873b. It should be noted that the amount of space added in Table II and Table III differs from the amount of space added in Table IV by a few bits, which is mainly caused by the line breaks in the plaintext data in the experiment. From an order of magnitude point of view, the amount of increase is the same, as shown in Fig. 11.

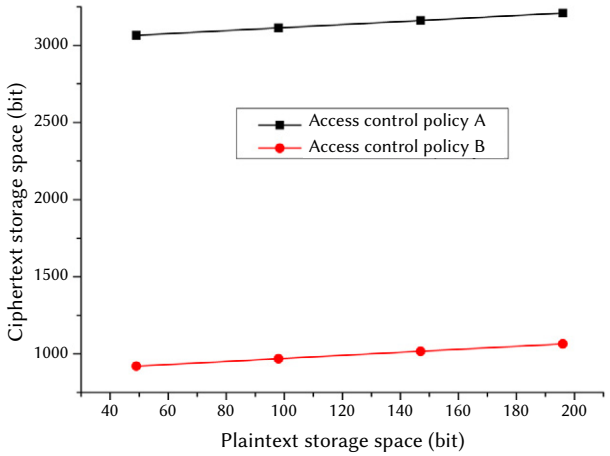


Fig. 11. The ciphertext storage space of different access control policies.

It is seen that when selecting encryption attributes and setting access control policies, to avoid occupying additional blockchain data storage space, the following three basic principles should be adhered to.

1. Choose as few encryption attributes as possible.
2. Configure access control policies as streamlined as possible.
3. For ciphertext data with large storage space, direct storage on the chain will take up too much space, and the IPFS system can be borrowed to relieve the pressure on blockchain storage.

E. Security Analysis

1. Data Access Control Policy Security

As described in section V.B, the access control right of the data collected by the security terminal is decided by the data access control policy file of the device. The CP-ABE encryption algorithm ensures that only users whose attributes and policies match exactly can decrypt the control policy file. In the scenario of consortium blockchain identity authentication and attributes issued by an authority, illegal users cannot steal confidential information. Meanwhile, the data access control file of the secure and trusted terminal can be dynamically adjusted according to the situation, such as changing the encryption key, updating the access control policy, etc., thereby ensuring the dynamic security of data access control.

2. Confidentiality of Private Data

This paper proposes a hybrid encryption scheme. The private data is encrypted with symmetric encryption algorithm, the key and device access control file are encrypted with CP-ABE algorithm, and strict access control strategy is set, which provides double insurance for the confidentiality of private data. As in section V.C, through data segmentation and private data encryption, the ciphertext is stored on the chain, which ensures the confidentiality of data under distributed data storage. The encryption key is stored in the access control policy file and encrypted based on CP-ABE algorithm, in this way, the data owner can better control the access authority of the data.

3. High Availability of Data

Both IPFS and blockchain adopt the principle of distributed technology, and the data collected by the IoT terminal is directly linked to the distributed storage. The technical characteristics of both determine the high availability of the system under single point or multi-point failure, and effectively improve the overall usability of the system.

4. Data Non-repudiation

In order to share data, publishers and users of data need to encrypt or decrypt twice, while encryption and decryption based on CP-ABE requires the support of user data attributes and logical relationship, i.e. access control policies. Therefore, the operation of data by both sides is undeniable and technically mutual trust. Specifically, distributed storage based on Fabric and IPFS ensures that data publishers cannot reject data on the blockchain. The adopted CP-ABE encryption algorithm ensures that data users obtain access rights through their own private key, and the operation of the key is undeniable. It solves the problems of data security and mutual trust in Agricultural IoT, and lays a foundation for the application of safe and reliable agricultural IoT data terminal in agricultural product quality and safety traceability system.

5. Anti-security Attack

The IoT often uses wireless communication for data transmission. If the private data is not encrypted, it can be easily eavesdropped by hackers. The privacy protection scheme proposed in this paper can resist eavesdropping attacks. At the same time, this paper encrypts the encryption key twice, which can effectively resist the plaintext key disclosure attack. For conventional IoT applications, data unauthorized access is the most common security attack or hidden danger. Using CP-ABE encryption algorithm to set fine-grained access control policies for data can effectively resist data unauthorized access attacks.

F. Performance Analysis

1. The Complexity of Key Management Is Significantly Reduced

The CP-ABE and DES hybrid encryption scheme designed in this paper realizes one-time encryption by users and flexible sharing among multiple users, which significantly reduces the complexity of key management in a symmetric cryptosystem. According to cryptographic theory, in a symmetric encryption system, if n users need to agree on a security key with each other, the number of keys required is n(n-1)/2. In this paper, the CP-ABE encryption algorithm is used to control access to the data encryption key. With n users participating, an access control policy is set for each user, that is, there are n decryption keys in total. Is the worst case. Therefore, the key management complexity is reduced from n(n-1)/2 to n.

2. Efficient and Flexible Access Control Policies

Data segmentation technology and CP-ABE encryption technology can protect data confidentiality and flexible access control, but the CP-ABE solution stores attributes and access control policies in ciphertext, which will increase the amount of ciphertext storage. It can be seen from Table II that when the access control policy A is used for encryption, the encrypted ciphertext of 49-bit plaintext data will become 3066 bits, which is 62.57 times the original. However, when the IPFS system is used to store it, the handle in the IPFS is stored on the blockchain, no matter how large the ciphertext data itself is, it will only occupy 46 bits of storage space.

According to the comparison data of IPFS storage space and ciphertext storage space shown in Fig. 12, taking the storage of 384848-bit files as an example, replacing the 387866-bit ciphertext storage with 46 bits will save 99.99% of the storage space. Obviously, this provides a new solution for setting more flexible and complex access control policies, while ensuring the efficiency of data storage.

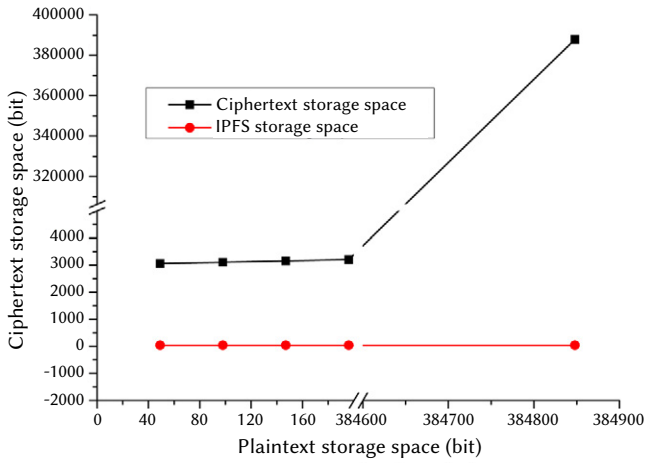


Fig. 12. Comparison of IPFS and ciphertext storage space.

3. It Has the Ability to Store and Expand the Big Data File of the Agricultural IoT

The agricultural IoT data includes not only the structured data of the experiment in this paper, but also unstructured data such as video, image, voice, GIS, etc. With the help of the IPFS file system, the corresponding smart contract can be developed to safely upload the above data to the chain.

VI. Conclusion

This paper studies the technical integration of agricultural IoT and blockchain, and designs a secure and trusted agricultural IoT blockchain terminal. With the help of CP-ABE and DES encryption algorithms, an access control and hybrid encryption scheme is designed to assure the security and authorized access control of data on the blockchain. Taking the data collection of the agricultural IoT production link as an example, the data segmentation, data encryption and access control scheme designed is verified. Through experimental verification, the terminal designed in this paper can be directly used as a node of the blockchain and IPFS to realize the release of collected data and the upload of files. However, the application scenarios of the agricultural IoT cover multiple links of agricultural production before, during and after production. The design of this system still needs to be continuously optimized according to specific business scenarios, which is also the main research direction of this work in the future. On the whole, the agricultural IoT blockchain terminal designed is a typical representative of the integrated application of blockchain and IoT technology, and has important research significance and application value.

Acknowledgment

This work was supported by the Project of Shandong Provincial Natural Science Foundation under Grant No.ZR2021QF056, Key R&D Program of Shandong Province (soft science project) under Grant No.2021RKL02002, Shandong social science planning and research project under Grant No.21CSDJ43, National Natural Science Foundation of China under Grant No. 62071320, Shandong federation of social sciences under Grant No. 2021-YYGL-32, and Tai'an Science and Technology Innovation Development Project under Grant No. 2020NS080.

References

[1] M. Torky, A. E. Hassanein, "Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges," *Computers and Electronics in Agriculture*, vol. 178, p. 105476, 2020, doi: 10.1016/j.compag.2020.105476.

[2] S. Raveena, A. S. Edward, "Secure b-iot based smart agriculture–a brief review," in *Journal of Physics: Conference Series*, vol. 1964, 2021, p. 042006, IOP Publishing.

[3] B. Bera, A. Vangala, A. K. Das, P. Lorenz, M. K. Khan, "Private blockchain-envisioned drones-assisted authentication scheme in iot-enabled agricultural environment," *Computer Standards & Interfaces*, vol. 80, p. 103567, 2022, doi: 10.1016/j.csi.2021.103567.

[4] M. Pincheira, M. Vecchio, R. Giaffreda, S. S. Kanhere, "Cost-effective iot devices as trustworthy data sources for a blockchain-based water management system in precision agriculture," *Computers and Electronics in Agriculture*, vol. 180, p. 105889, 2021, doi: 10.1016/j.compag.2020.105889.

[5] T. H. Pranto, A. A. Noman, A. Mahmud, A. K. M. B. Haque, "Blockchain and smart contract for iot enabled smart agriculture," *PeerJ Computer Science*, vol. 7, p. e407, 2021, doi: 10.7717/peerj-cs.407.

[6] L. Hang, I. Ullah, D. Kim, "A secure fish farm platform based on blockchain for agriculture data integrity," *Computers and Electronics in Agriculture*, vol. 170, p. 105251, 2020, doi: 10.1016/j.compag.2020.105251.

[7] O. Lamtzidis, D. Pettas, J. Gialelis, "A novel combination of distributed ledger technologies on internet of things: Use case on precision agriculture," *Applied System Innovation*, vol. 2, no. 3, p. 30, 2019.

[8] W. Keke, C. Zhide, X. Jian, "Efficient traceability system for quality and safety of agricultural products based on consortium blockchain," *Journal of Computer Applications*, vol. 39, no. 8, p. 2438, 2019.

[9] Y. Li'na, Z. Guofeng, J. Jingdun, G. Wanlin, Z. Ganghong, T. Sha, "Modern agricultural product supply chain based on block chain technology," *Nongye Jixie Xuebao/Transactions of the Chinese Society for Agricultural Machinery*, vol. 48, pp. 387–393, 2017.

[10] S. Namasudra, G. C. Deka, P. Johri, M. Hosseinpour, A. H. Gandomi, "The revolution of blockchain: State-of-the-art and research challenges," *Archives of Computational Methods in Engineering*, vol. 28, no. 3, pp. 1497–1515, 2021.

[11] A. A. Khan, M. Uddin, A. A. Shaikh, A. A. Laghari, A. E. Rajput, "Mf-ledger: Blockchain hyperledger sawtooth-enabled novel and secure multimedia chain of custody forensic investigation architecture," *IEEE Access*, vol. 9, pp. 103637–103650, 2021, doi: 10.1109/ACCESS.2021.3099037.

[12] G. Zhang, X. Chen, B. Feng, J. Wen, "Research on a safe and reliable agricultural product traceability system driven by permissioned blockchain technology," in *The International Conference on Image, Vision and Intelligent Systems (ICIVIS 2021)*, 2022, pp. 955–966, Springer.

[13] M. Uddin, "Blockchain medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry," *International Journal of Pharmaceutics*, vol. 597, p. 120235, 2021.

[14] M. Jemel, A. Serhrouchni, "Decentralized access control mechanism with temporal dimension based on blockchain," in *14th IEEE International Conference on Ebusiness Engineering, ICEBE 2017, Shanghai, China, November 4-6, 2017*, 2017, pp. 177–182, IEEE Computer Society.

[15] Z. Zhang, X. Ren, "Data security sharing method based on CP-ABE and blockchain," *Journal of Intelligent & Fuzzy Systems*,vol. 40, no. 2, pp. 2193–2203, 2021, doi: 10.3233/JIFS-189318.

[16] X. Wang, X. Jiang, Y. Li, "Model for data access control and sharing based on blockchain," *Ruan Jian Xue Bao/Journal of Software*, vol. 30, no. 6, pp. 1661–1669, 2019.

[17] Y. Zhang, B. Li, B. Liu, J. Wu, Y. Wang, X. Yang, "An attribute-based collaborative access control scheme using blockchain for iot devices," *Electronics*, vol. 9, no. 2, p. 285, 2020.

[18] G. Zhang, X. Chen, B. Feng, X. Guo, X. Hao, H. Ren, C. Dong, Y. Zhang, "BCST-APTS: blockchain and CP-ABE empowered data supervision, sharing, and privacy protection scheme for secure and trusted agricultural product traceability system," *Security and Communication Networks*, vol. 2022, pp. 2958963:1–2958963:11, 2022, doi: 10.1155/2022/2958963.

[19] A. Sahai, B. Waters, "Fuzzy identity-based encryption," in *International Conference on Theory & Applications of Cryptographic TechniquesAnnual*, 2005, pp. 457–473, Springer.

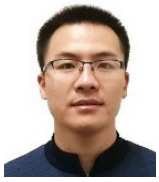
[20] V. Goyal, O. Pandey, A. Sahai, B. Waters, "Attribute- based encryption

for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, October 30 - November 3, 2006*, 2006, pp. 89–98, ACM.

[21] J. Bethencourt, A. Sahai, B. Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE symposium on security and privacy (SP'07)*, 2007, pp. 321–334, IEEE.

[22] L. Zhang, W. Zeng, Z. Jin, Y. Su, H. Chen, "A research on traceability technology of agricultural products supply chain based on blockchain and ipfs," *Security and Communication Networks*, vol. 2021, 2021.

[23] B. W. John Bethencourt, Amit Sahai, "Ciphertext- policy attribute-based encryption," *[Online]*, vol. 2021, 2021.



Guofeng Zhang

He was born in June 1986. He graduated from China Agricultural University with a doctor's degree in 2020 and North China University of technology with a master's degree in 2013. At present, he works in Taishan University and is now a lecturer. The main research fields are blockchain, Internet of things, information security, etc.

Xiao Chen

She was born in October 1986 and graduated from China Agricultural University with a master's degree in 2012. Since 2012, she has been working in Taishan University and is now a lecturer. At present, the main research directions are digital economy and blockchain technology.

Lei Zhang

He was born in June 1983, graduated from East China Normal University in Shanghai 2009, with a master's degree. I have been working in Shandong Academy of Macroeconomic Research since 2010.Now I am the deputy director of the investment and Financing Policy Research Institute.My main research directions are digital economy, industrial economy, etc. I have published 1 monograph, 12 journal articles, presided over and completed 4 provincial social science projects, and won 6 provincial awards such as the provincial social science outstanding achievement award.

Bin Feng

He received the BS degree in Computer Science and Technology in 2002 from the LiaoCheng University, Shandong, China, and the MS degree in software engineering in 2006 from the Dalian University of Technology, Dalian, China. He has been an assistant in TaiShan University among 2002–2004. He is currently a full engineer of Computer Science at Dalian University of Technology, Dalian, China, since 2006. Since 2011, he is currently pursuing his PhD degree in computer software and theory from the Dalian University of Technology, Dalian, China. His research interests include data hiding, image processing, network and information security.

Xuchao Guo

He received Bachelor degree in Computer Science in 2015 and his Master's degree in 2018 from Shandong Agricultural University, China. He is currently Ph.D. student in the College of Information and Electrical Engineering, China Agricultural University, China. He is mainly engaged in natural language processing and knowledge graph. His research interests include: deep learning, natural language processing, computer vision, complex network analysis.

Jingyun Liang

She graduated from Shandong University in 2005 with a master's degree in Applied Chemistry. She worked in Shandong Agricultural University from 2005 to 2011 and has worked in the Institute of agricultural quality standards and testing technology of Shandong Academy of Agricultural Sciences since 2011. The main research direction is the analysis and risk assessment of toxins and pesticide residues in agricultural products. Presided over one sub project of the national risk assessment project and two projects of Shandong Provincial Department of science and technology, published 5 SCI papers and applied for more than 10 invention patents.

Yanan Zhang

She was born in Heze, Shandong, China, in 1997.She is currently pursuing a master's degree, Majored in electronic information in School of Information Science and Engineering, Jinan University, Jinan, Shandong, China. From 2020 to 2022, She has been researching on blockchain techniques, especially on fabric. Her research interests include blockchain data security, privacy protection.