Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 162 (2019) 82–87

Procedia Computer Science

www.elsevier.com/locate/procedia

7th International Conference on Information Technology and Quantitative Management (ITQM 2019)

# Blockchain based Data Distribution and Traceability Framework in the Electric Information Management System

Mengchen Cai*, Ming Li, Wanwan Cao

*Department of Information Communication, State Grid Anhui Electric Power Company, Hefei, Anhui, China*

**Abstract**

Blockchain technology is playing an increasingly important role in the Management Information System especially in the data security aspect. In this paper, we propose a blockchain based system for the data distribution and traceability analysis in Electric Management Information System (EMIS). The blockchain and smart contract is studied to ensure the security of data share in the system. The experimental results indicate that the proposed demo system can efficiently support the data share and supply the undeniable traceability services in EMIS.

*Keywords:* Electric Management Information System; Blockchain; Data Distribution; Traceability

## 1. Introduction

Electric Information Management System is playing an important role in the security of national energy supply. There is a lot of sensitive data in the system and it is necessary to control and track the access of these datasets. Along with the development of IT infrastructure, information sharing becomes more and more convenient, however it also bring the problem of data security. To protect the data from abuse, security distribution and traceability framework should be studied. For example, if the sensitive information leaks out, we have to know where the problem is so we can identify the responsible personal and fix it next time.

Blockchain has been applied in many data security related applications. As a decentralized framework, it can record the data transmission in an undeniable way and provide the traceability information. In this paper, we apply the blockchain technology to implement a data distribution and traceability framework for the electric company. In the proposed framework, sensitive data is encrypted and stored in IPFS (InterPlanetary File System).

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000 .
*E-mail address:* caimc0615@ah.sgcc.com.cn.

10.1016/j.procs.2019.11.261

Only the key is transmitted from the sender to receiver and it is record in the blockchain as a transaction. The receiver can only access the data through a predefined smart contract in the blockchain system and this action is also recorded for the traceability analysis. Through the blockchain system, we can control the data distribution and find out how it is accessed by the receivers, which provides better control for the data in electric information management system.

The rest of paper is structured as follows. Related work is introduced in section 2. Section 3 describes the proposed methodology in details. Section 4 demonstrates the system implementation and experimental results. Finally section 5 concludes the whole paper.

## 2. Related Work

### *2.1. Data distribution and traceability analysis*

Along with the development of IoT and 5G, increasing number of sensitive datasets are collected especially for Electric Management Information System, in which the security of data transmission and sharing is an essential task for the overall stable operation of the system [1]. Pirbhulal et al. [2] studied the security data transmission framework for wearable healthcare system to supply a trade-off between security and resource optimization. Du et al. [3] proposed a unified privacy protection system for video surveillance data and designed a private preserving video encoding and storage algorithm.

### *2.2. Blockchain technology*

Recent years, decentralized data security schema is developed rapidly. The blockchain has been applied in many applications to improve the data security such as IoT [4]. Zhu et al. [5] utilized blockchain for cloud data management based on higher level of voting authorization. Liu et al. [6] employed blockchain and smart contract to data carrier applications in IoT environment. Tian et al. [7] proposed a secure digital evidence framework using blockchain to solve big data and privacy challenges with a loose coupling design. Muzammal et al. [8] improved the database to supply data integrity and reliability by blockchain. Feng et al. [9] introduced blockchain to crowed sourcing applications to support a liveness, decentralization, and fault tolerance services. Shrestha [10] proposed a type of blockchain to resolve critical message dissemination issues in Vehicular Ad-ho Networks. For Electric power related applications, blockchain is used by Zhang et al. (2019) to create a decentralized and secure keyless signature scheme for smart grid. However, the blockchain based data transmission and traceability analysis in EMIS is not intensively studied, and this paper will focus on the problem.

## 3. Methodology

### *3.1. Overall framework*

The overall structure of proposed framework is described in Figure 1. First the data is stored in the IPFS which can supply the access to the required data through a hash code. All data is encrypted so that we can control its accessibility just with the key, which can speed up the efficiency of data distribution. A blockchain system is used to transmit the access key of the data. Besides, the data can only be read through a smart contract system connected to the blockchain. Based on the information in the blockchain, we can implement the accessibility analysis for all data in the system.

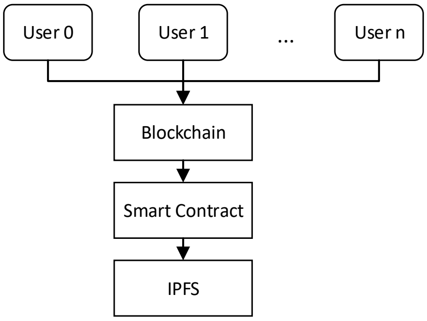


Fig. 1. Overall framework

### *3.2. Data distribution based on Blockchain*

Each user in the proposed system can send or receive data to or from others. However, the data is not directly transmitted between users (A and B for example) but through the following three steps.

1) The sensitive data is first encrypted and stored in the IPFS by user A. Everyone can download the encrypted data according to a hash code of the data, but only the one has the key can read the data.

2) If A wants to send the data to B, he or she writes a record in the blockchain that indicates A has sent a data D to B. This record also contains the key to the data D which is encrypted by B's public key, so that only B can get the key and to read the data D from A.

3) A Consensus Protocol is selected to make sure the non-repudiation of the data transmission records. In this framework, Practical Byzantine Fault Tolerance (PBFT) Consensus Protocol is selected to improve the system performance. Compared with the widely applied PoW or PoS Consensus Protocols, PBFT can run without the tokens /coins which is not necessary in the Electric Information Management scenario. Also the PBFT can record a new transaction in around 2-5 seconds to support a near real time data distribution.

The blockchain based data distribution system can ensure that A has tried to send the data to B. If B read the data can be further controlled by the smart contract.

### *3.3. Data access with Smart contract*

Smart contract is a protocol that can be performed without third parties in a trackable and irreversible way. Although smart contract has been proposed by Nick Szabo around 1997, it is recently implemented based on blockchain technologies that implement the requirements to create a practical application. The smart contract is also known as the feature of blockchain 2.0.

In this paper, we create a smart contract to control the data accessibility of the sensitive data in Electric information management system. The proposed smart contract mainly deals with data read, which is a relative simple operation and can be easily verified. First all users in the system sign a smart contract that can generate a record when a user reads the data. This smart contract is record in the blockchain and send to each user in the system. For new user, he or she also signs the contract and update the contract accordingly.

When the user B receive the data and key from user A, B will run the smart contract to read the data. The smart contract supply the encrypt and decrypt services in the system, in another word we can only read the data through the smart contract even if we know the key. The generated smart contract will decrypt the data and write a record in the blockchain indicate when and who reads the data.

The data owner or sender can also terminate the accessibility to a dataset by updating the smart contract.

### 3.4. Graph based traceability analysis

The blockchain contains all information related to sensitive data distribution and accessing records. However, the information is included in many different blocks which is difficult to analysis and querying. In the proposed framework, we extract the traceability information from blockchain and stored to graph database for further analysis.

In the graph database, the nodes represent the users in the system, and the edges represent a transmitted data between users. The edge is directed and contains the attributes about the data, time and access information from receivers. Based the traceability graph, we can easily identified the sources and targets of the data and demonstrate the dataflow, which is useful to analysis and control the data spread in the system.

Another application for the graph based traceability analysis is abnormal detection. Since the business in electric information management system is usually periodical or similarity to the history, we implement the abnormal detection based on the graph similarity calculation. First, for each dataset, a traceability graph is generated from graph database. Then, the distances between nodes and edges are defined based on their attributes. For different applications, the attributes of nodes and edges are different and the distances should be adjusted accordingly. Next, the overall distance between two graphs can be calculated by graph similarity algorithms such as Nested Earth Mover's Distance. Finally, the traceability graphs can be classified and the outliers will be detected as the abnormal ones.

## 4. Implementation and Results

### 4.1. Blockchain system

To implement the proposed data distribution and traceability system, we create ten deployment unit (DU) in the company internet located in four physics places.

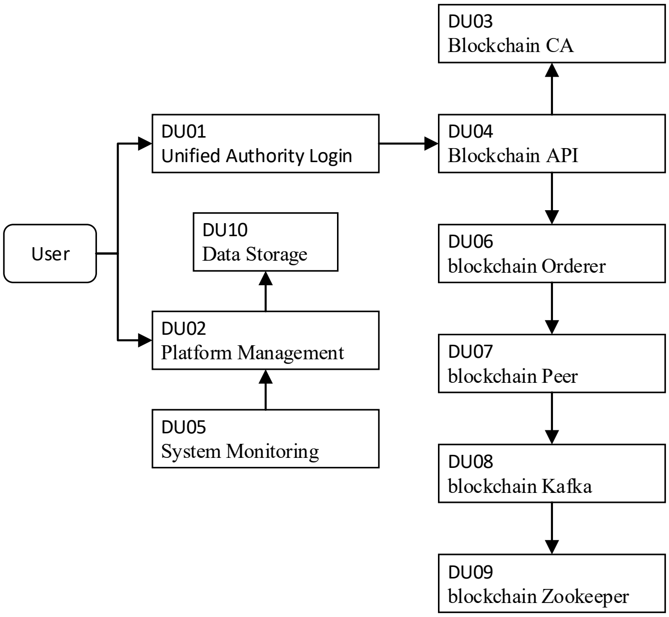


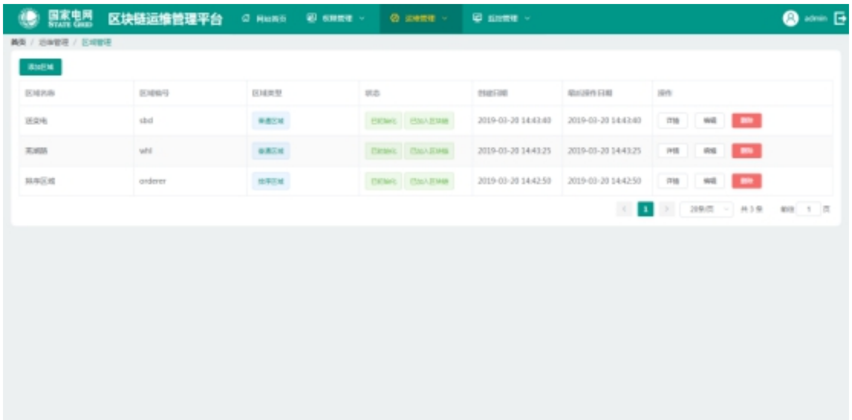
Fig. 2. System implementation framework

DU01 is unified authority login deployment unit, DU02 is platform management deployment unit, DU03 is the blockchain CA deployment unit, DU04 is the blockchain API deployment unit, DU05 is the monitoring deployment unit, DU06 is the blockchain Orderer deployment unit, DU07 is the blockchain Peer deployment unit, DU08 is the blockchain Kafka deployment unit, DU09 is the blockchain Zookeeper deployment unit, and DU10 is data storage deployment unit. These DUs are running on virtual machines with 8 2.6GHz cores, 16G memory, 500G disk and 2 1000M network connections. The DU10 data storage unit contain extra 16T disk space. All DUs are configured with CentOS 7.0, MySQL is selected as the database and WEBLOGIC 10g is used as the application server.

The proposed frame is implemented based on Ethereum which supplies an interface to integrate the blockchain and smart contract in the system.

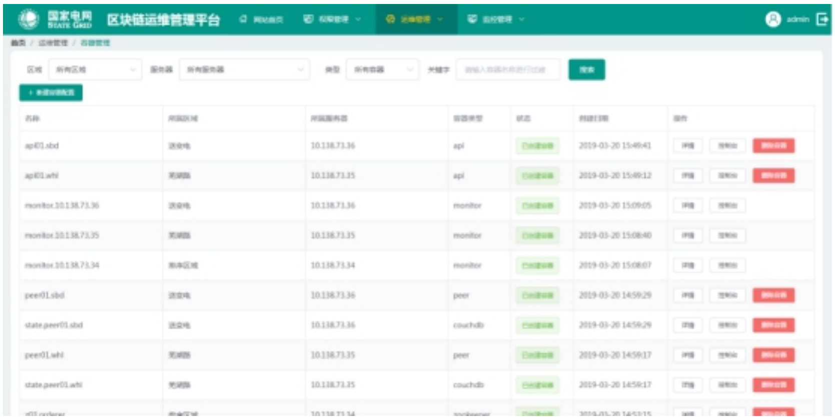
### 4.2. System GUI

A web based system is implemented to configure and manage the blockchain based data distribution framework. We can upload data and download data in the system. Also to check the traceability information of the data. Figure 3 and Figure 4 gives some screenshots of the implemented system.



| 区域名称 | 区域编号 | 区域类型 | 状态 | 创建日期 | 最后操作日期 | 操作 |
|---|---|---|---|---|---|---|
| 送变电 | sbd | [illegible] | [illegible] | 2019-03-20 14:43:40 | 2019-03-20 14:43:40 | 详情 编辑 删除 |
| [illegible] | whl | [illegible] | [illegible] | 2019-03-20 14:43:25 | 2019-03-20 14:43:25 | 详情 编辑 删除 |
| 排序区域 | orderer | 排序区域 | [illegible] | 2019-03-20 14:42:50 | 2019-03-20 14:42:50 | 详情 编辑 删除 |

Fig. 3. Implemented GUI of the Blockchain based data distribution framework



| 名称 | [illegible] | [illegible] | [illegible] | 状态 | [illegible] | 操作 |
|---|---|---|---|---|---|---|
| api01.sbd | 送变电 | 10.138.73.36 | api | [illegible] | 2019-03-20 15:49:41 | [illegible] |
| api01.whl | [illegible] | 10.138.73.35 | api | [illegible] | 2019-03-20 15:49:12 | [illegible] |
| monitor.10.138.73.36 | 送变电 | 10.138.73.36 | monitor | [illegible] | 2019-03-20 15:09:05 | [illegible] |
| monitor.10.138.73.35 | [illegible] | 10.138.73.35 | monitor | [illegible] | 2019-03-20 15:08:40 | [illegible] |
| monitor.10.138.73.34 | 排序区域 | 10.138.73.34 | monitor | [illegible] | 2019-03-20 15:08:07 | [illegible] |
| peer01.sbd | 送变电 | 10.138.73.36 | peer | [illegible] | 2019-03-20 14:59:29 | [illegible] |
| state.peer01.sbd | 送变电 | 10.138.73.36 | couchdb | [illegible] | 2019-03-20 14:59:29 | [illegible] |
| peer01.whl | [illegible] | 10.138.73.35 | peer | [illegible] | 2019-03-20 14:59:17 | [illegible] |
| state.peer01.whl | [illegible] | 10.138.73.35 | couchdb | [illegible] | 2019-03-20 14:59:17 | [illegible] |
| [illegible] | 排序区域 | 10.138.73.34 | zookeeper | [illegible] | 2019-03-20 14:53:15 | [illegible] |

Fig. 4. Data access records in the system

## 5. Conclusions

In this paper, we implement a blockchain based system for the data distribution and traceability analysis in Electric Management Information System. The proposed framework takes advantages of blockchain and smart contract to ensure the security of data share in the system. The implemented demo system verify the efficiency of proposed framework.

## References

[1] Christos Stergiou, Kostas E. Psannis, Brij B. Gupta, Yutaka Ishibashi, Security, privacy & efficiency of sustainable Cloud Computing for Big Data & IoT, Sustainable Computing: Informatics and Systems, Volume 19, 2018, Pages 174-184,

[2] Sandeep Pirbhulal, Oluwarotimi Williams Samuel, Wanqing Wu, Arun Kumar Sangaiah, Guanglin Li, A joint resource-aware and medical data security framework for wearable healthcare systems, Future Generation Computer Systems, Volume 95, 2019, Pages 382-391,

[3] Ling Du, Wei Zhang, Huazhu Fu, Wenqi Ren, Xinpeng Zhang, An efficient privacy protection scheme for data security in video surveillance, Journal of Visual Communication and Image Representation, Volume 59, 2019, Pages 347-362,

[4] Sana Moin, Ahmad Karim, Zanab Safdar, Kalsoom Safdar, Ejaz Ahmed, Muhammad Imran, Securing IoTs in distributed blockchain: Analysis, requirements and open issues, Future Generation Computer Systems, Volume 100, 2019, Pages 325-343,

[5] Liehuang Zhu, Yulu Wu, Keke Gai, Kim-Kwang Raymond Choo, Controllable and trustworthy blockchain-based cloud data management, Future Generation Computer Systems, Volume 91, 2019, Pages 527-535,

[6] Xiaolong Liu, Khan Muhammad, Jaime Lloret, Yu-Wen Chen, Shyan-Ming Yuan, Elastic and cost-effective data carrier architecture for smart contract in blockchain, Future Generation Computer Systems, Volume 100, 2019, Pages 590-599,

[7] Zhihong Tian, Mohan Li, Meikang Qiu, Yanbin Sun, Shen Su, Block-DEF: A secure digital evidence framework using blockchain, Information Sciences, Volume 491, 2019, Pages 151-165,

[8] Muhammad Muzammal, Qiang Qu, Bulat Nasrulin, Renovating blockchain with distributed databases: An open source system, Future Generation Computer Systems, Volume 90, 2019, Pages 105-117,

[9] Wei Feng, Zheng Yan, MCS-Chain: Decentralized and trustworthy mobile crowdsourcing based on blockchain, Future Generation Computer Systems, Volume 95, 2019, Pages 649-666,

[10] Rakesh Shrestha, Rojeena Bajracharya, Anish P. Shrestha, Seung Yeob Nam, A new-type of blockchain for secure message exchange in VANET, Digital Communications and Networks, 2019, in press

[11] Hongwei Zhang, Jinsong Wang, Yuemin Ding, Blockchain-based decentralized and secure keyless signature scheme for smart grid, Energy, Volume 180, 2019, Pages 955-967,.