

Online test and management system using blockchain network

Seung Jae Pee*, Eung Seon Kang*, Jae Geun Song*, Ju Wook Jang*

*Department of Electronic Engineering, Sogang University, 35, Shinsu-dong, Mapo-gu, Seoul, South Korea

paul_0238@naver.com, kes617@naver.com, 1080skj@gmail.com, jjang@sogang.ac.kr

Abstract— The current online test service only focused on convenience, but did not offer a solution to securing reliability. Also current online test service, which are centralized server storage and management methods, will not be able to maintain such systems in the event of SoF(Single-point of Failure) or physical problems. In this paper, we discuss online test and management system using private blockchain and CP-ABE(Ciphertext-Policy Attribute-Based Encryption, create an 'Access tree' based on the user attribute to encrypt the information) algorithm. In the system, the private blockchain network is constructed with the nodes of the system manager, examiners, and examinees, and each node has different authority. Since the data encrypted by the CP-ABE algorithm cannot be decrypted without the corresponding attribute, it is impossible to read or modify the data.

Keywords— Online Test System, Blockchain, CP-ABE, Smart Contract, Application Security

I. INTRODUCTION

Various tests are being conducted online with the Internet's penetration. However, the current online test service only focused on convenience, but did not offer a solution to securing reliability. Also current online test service, which are centralized server storage and management methods, will not be able to maintain such systems in the event of SoF(Single-point of Failure) or physical problems. Test personnel or attackers may commit cheating, such as forgery, falsify, or deleting test content or result. To address these problems, we discuss online test and management system that enable security, reliability, and privacy based on a blockchain network.

In this paper, we discuss online test and management system using private blockchain and CP-ABE(Ciphertext-Policy Attribute-Based Encryption, create an 'Access tree' based on the user attribute to encrypt the information) algorithm. In the system, the private blockchain network is constructed with the nodes of the system manager, examiners, and examinees, and each node has different authority. And the system manager manages the transaction generation and query authority of other nodes by using CP-ABE algorithm. First, a public key, a private key, and an ID are generated using the user's personal information in the blockchain network created by the system manager node. At this time, the first node created has no attribute. The examiner can receive the 'examiner' attribute with the approval of the manager node

and has the authority to record the problem in the form of transaction in the blockchain network. The examinee also receives the 'examinee' attribute from manager node to take test, then saves encrypted data, which contains 'examinee' and 'course' attributes on a blockchain. After that, the system manager scored through the smart contracted answers and the examinees can check the scoring results by querying transaction. Since the data encrypted by the CP-ABE algorithm cannot be decrypted without the corresponding attribute, it is impossible to read or modify the data.

The rest of the paper is organized as follow. In Section II, we describe the properties of blockchain and CP-ABE. Section III explains the process of online test and management system, and Section IV concludes the paper.

II. BACKGROUND

A. Blockchain

The blockchain is a P2P-based distributed data network system. Because the blocks are grouped into chains, they are named as blockchain. In the blockchain, all users participating in the network distribute and store history data in block format, which is a set of transactions. Since each node has a single secret key and a public key, it is possible to perform a digital signature on the transaction using the secret key and the hash function. Each node uses the public key to verify whether the subject of the digital signature actually signed the transaction[1]. The block containing this transaction has a structure of "chains" that are continuously connected along the time flow after being made at a specific cycle. Because all users hold transaction history, every user can verify the transaction history by checking the ledgers they hold. Therefore, transactions that are not validated can't be stored in the block. Thus, blockchain has three characteristics: data integrity, security, and decentralization[2].

B. CP-ABE

CP-ABE is encryption method proposed by Bethencourt[3] in 2007, in which the access tree is used to encrypt the data itself, not the access tree is in the user's private key. In order to decrypt the encrypted data in the original text, a private key generated from the access tree created based on the attribute set of the user is required. The data can be decrypted only if the corresponding private key meets the access tree of the data.

III. ONLINE TEST AND MANAGEMENT SYSTEM USING BLOCKCHAIN

A. Online Test and Management System Process

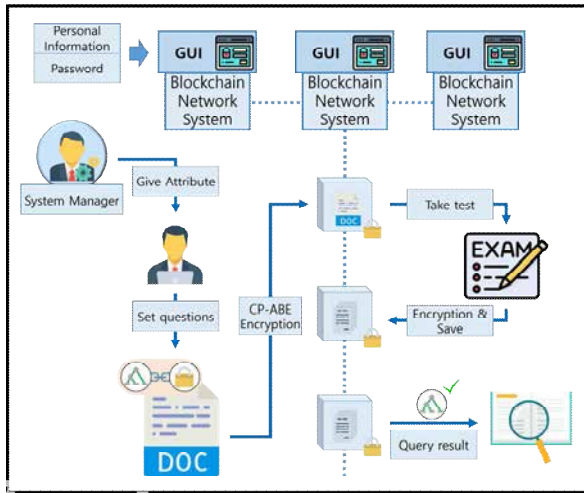


Figure 1. Process of online test and management system

Figure 1 shows the process of online test and management system. The nodes enter the ID and Password in the GUI, then they are given the public key and private key, and join the blockchain network. Through the GUI, each node can be provided with services such as write test questions, take test, and so on. The system manager creates the blockchain network, assigns attributes to each node, and acts as an administrator of the online test and management system. The examiner node to which the attribute is assigned writes a test question, signs it with the private key, restricts the access authority using the CP-ABE algorithm, and saves it in the blockchain network. At the test time, the system manager node reads the test questions recorded on the blockchain network and saves them to the blockchain network by CP-ABE so that the examinee nodes can access them. Examinee nodes will take the test and write their answers to the blockchain network with CP-ABE, so that only themselves and system manager can query them. After being scored by the system manager, the examinee nodes will be able to query the results.

B. Examiner Nodes

Figure 2 shows the process in which examiner node receives the attributes of the 'examiner' from the system manager, writes the test questions and saves them in the blockchain network. First, examiner participates in the blockchain network by entering ID and password in the GUI, and receives the public key and the private key. The system manager confirms participation of the examiner node and assigns the 'subject' and 'examiner' attributes to the node. Examiner node who is given the attribute writes the problem, signs it with his private key. Then, encrypts it with the 'subject' and 'examiner' attribute, and saves it in the blockchain network. At this time, the access binary tree used for CP-ABE is shown in the right of Figure 2. If there are

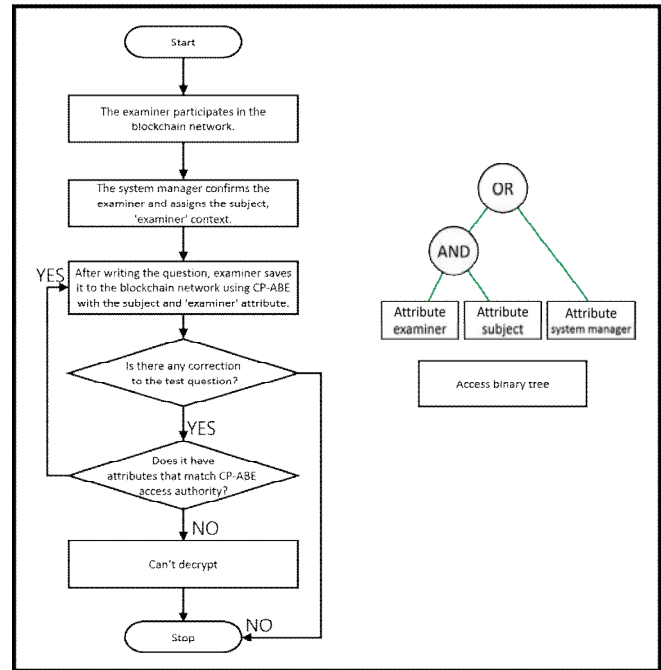


Figure 2. Process of examiner node's work

modifications to the test question, examiner node accesses the problem saved in the blockchain network. If there is no attribute to access the CP-ABE encrypted data, the record cannot be read because it cannot be decrypted. When the test question is modified, the version recorded in the transaction data is also modified and save it in blockchain network.

C. Examinee Nodes

Figure 3 shows the process in which the examinee node receives the 'examinee' attributes from the system manager and takes the test, then saves the answer in blockchain network as form of transaction. The examinee node also enters the ID and password in the GUI and participates in the blockchain network and receives public key and private key, as in the case of the examiner node. The system manager confirms participation of the examinee node and assigns the 'subject' and 'examinee' attributes to the node. When the test time, the system manager query the latest version of the test questions saved on the blockchain network, and modifies the access binary tree used for CP-ABE encryption as shown in the upper right of Figure 3. So that examinee nodes will be able to take test. Other nodes with different subject attribute or no examinee attribute cannot be take test because they can't decrypt CP-ABE encrypted transactions. When the examinee node writes an answer, encrypts it using the access binary tree as shown in the lower right of Figure 3. This allows the transaction author and the system manager to verify the answer.

D. Giving Score

Figure 4 shows how the system manager scores the answers submitted by examinee nodes using the smart contract, and the examinee reviews the scoring results. The examiner writes the

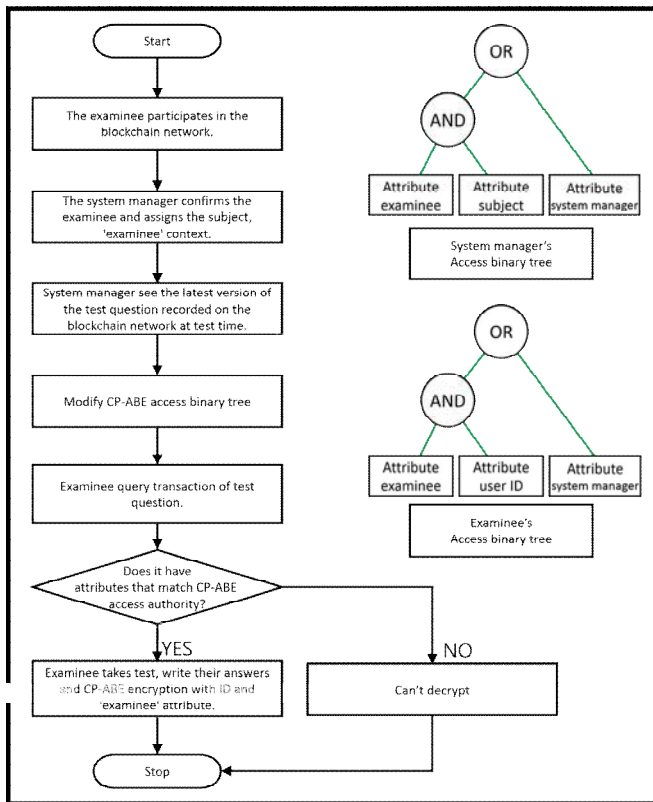


Figure 3. Process of examinee node's work

test answer as a smart contract in the form of a function, and saves it in the blockchain network with CP-ABE. At this time, the access binary tree used for CP-ABE encryption is shown in Figure 2. After the end of the test period, the system manager will query the answer written by the examinees. When the solution of the problem is called as smart contract function as an input value, the scoring result (test score) is output. This result is saved in the blockchain network by CP-ABE encryption with the examinee's ID and 'examinee' attributes. Each examinee node will be able to query the scoring results by his ID and 'examinee' attribute.

IV. CONCLUSIONS

In this paper, we applied the CP-ABE to the online test and management system using blockchain to efficiently control access authority. All data sent from the examiner node and the examinee node are saved on an immutable and distributed data storage called blockchain[4]. A node that doesn't have access authority will not be able to query the data, but can verify that it had been modified. Thus, it provides a data integrity, authentication and reliable system. You can also apply this system to other applications with many N:N connections. We believe that it allows people to be more comfortable and trustable.

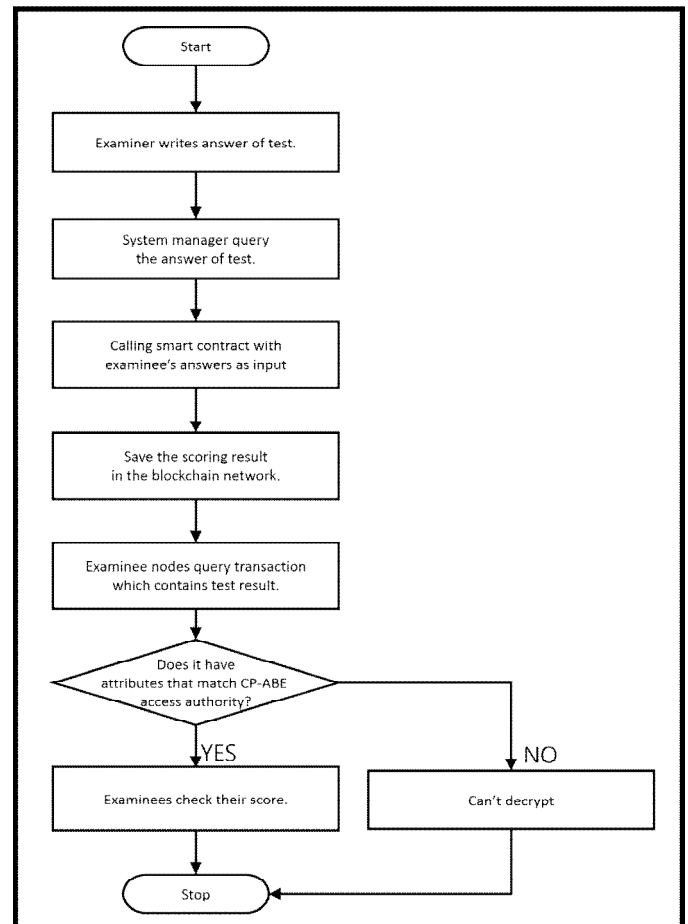


Figure 4. Process of scoring test

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(NRF-2016R1D1A1B01009027).

REFERENCES

- [1] Nakamoto Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008
- [2] Seung Jae Pee, Jong Ho Nang, Ju Wook Jang (2018). "A Simple Blockchain-based Peer-to-Peer Water Trading System Leveraging Smart Contracts". [Online]. Available: <https://csce.ucmss.com/cr/books/2018/ConferenceReport?ConferenceKey=ICM>
- [3] Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy, pp. 321–334. IEEE Computer Society, Los Alamitos (2007)
- [4] M. Crosby, Nachiappan, P. Pattanayak, S. Verma and V.Kaly Sutardja Center for Entrepreneurship&Technology, <http://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf> (accessed June 20, 2016)



Seung Jae Pee was born on September 16, 1992 in Korea. He graduated in 2018 after majoring in electronic engineering at Sogang University in 2011. And he has been working on master's degree at Sogang University in Mobile Network Laboratory since 2018.



Eung Seon Kang was born on June 17, 1992 in Korea. He graduated in 2018 after majoring in electronic engineering at Sogang University in 2012. And he has been working on master's degree at Sogang University in Mobile Network Laboratory since 2018.



Song Jae Geun was born on January 8, 1995 in Korea. He graduated in 2018 after majoring in electronic engineering at Sogang University in 2013. And he has been working on master-doctor degree at Sogang University in Mobile Network Laboratory since 2018.



Ju Wook Jang received a B.S. degree in Electronic Engineering from Seoul National University, Seoul, Korea, an M.S. degree in Electrical Engineering from the Korean Advanced Institute of Science and Technology (KAIST), and a Ph.D. in Electrical Engineering from the University of Southern California (USC), Los Angeles, USA. From 1985 to 1988 and 1993 to 1994, he worked with Samsung Electronics, Suwon, Korea, where he was involved in the development of a 1.5-Mb/s video codec and a parallel computer. Since 1995, he has been at Sogang University, Seoul, Korea, where he is currently a professor. His current research interests include WiMAX protocols, mobile networks and next-generation networks. He received the LG Yonam overseas research grant in 2001. He has also built systems for videoconferencing, streaming, home networks and ad hoc networks using protocols like RTP, SIP, multicast and IPv6.