Ilkogretim Online - Elementary Education Online, 2021; 20 (3): pp. 716-721
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.03.75

A Blockchain-based Untact Education System for the Post-COVID-19 Era

Donghyeok Lee, *Science Technology Society Research Center, Jeju National University*
Namje Park, *Department of Computer Education, Teachers College, Jeju National University 61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 63294, Korea, namjepark@jejunu.ac.kr*
*Corresponding author

Abstract. With the advent of the post-COVID-19 era, the existing educational environment is at the point of transition to an untact-based educational environment. The current online education system has a limitation in safely providing the untact education system. We proposed an untact education system based on blockchain. Through the proposed method, learning contents and results can be safely stored in the blockchain. In addition, integrity damage due to data manipulation can be prevented. In particular, the efficiency of learning can be improved through behavioral analysis in the learning process, and the privacy of learners is protected by masking face recognition data. In the untact education environment, privacy exposure to learners may occur, and various information such as facial recognition data and test evaluation data may be exposed. Blockchain can safely protect against these vulnerabilities. As an advantage of the proposed method, the teacher can take appropriate action by grasping the learner's concentration through real-time behavior analysis. It also generates warnings when learners take inappropriate actions. These advantages increase the efficiency of untact education by enabling timely education.

Keywords: Untact Education, Blockchain, Privacy Protection, LMS, Behavior Analysis

Received: 08.12.2020 Accepted: 17.01.2021 Published: 05.02.2021

Introduction

With the recent COVID-19 outbreak, the importance of distance learning is increasing. In the aftermath of COVID-19, many schools are offering online classes. Until now, some classes have been conducted online, but most of them play pre-recorded videos. However, the untact educational environment is fundamentally different from these past online classes. In an untact educational environment, teachers and students must participate in real time, and students' reactions and participation levels must be checked in real time and reflected in class. Since the COVID-19 outbreak, these changes have come suddenly and are currently not fully responded. Therefore, there is a growing concern and awareness that online classes are poor, and research on such an untact education system is urgent. In the untact educational environment, measures for privacy protection or information security are required. When a student takes classes in real time, information may be collected in the learning system as needed. In order to detect inappropriate behavior in the course of the class, not only identity information such as the student's name and school, but also various information such as facial information and motion can be collected and analyzed through image analysis to identify class concentration. If so, appropriate action may be taken. Video surveillance is necessary for analysis of learner's attendance and learning attitudes, but this can infringe on learner's personal privacy, and if such information is exposed to the outside through hacking, it can lead to serious personal information exposure. On the other hand, it is also possible to arbitrarily manipulate academic participation videos or scoring results for the purpose of illegally manipulating academic achievement. In particular, this problem is more serious in a public cloud environment. Learning data may be exposed by a cloud service provider or a third party, and personal information may be infringed. Also, even if end-to-end encryption is applied, manipulation of learning data is not easy to detect. Therefore, countermeasures to these problems are essential in a cloud-based untact education system environment. To solve these problem, we propose a blockchain-based untact education system. Blockchain can fundamentally prevent data manipulation, making it suitable for online learning systems that need to ensure integrity. The method proposed in this paper has the advantage that it is impossible to manipulate learning information by using a blockchain, and by using a variable blockchain, it is possible to mask the user's face information, thereby protecting the privacy safely.

1. Related research

Online education has a lot of potential because it is not restricted by space, and it will be an essential element in the untact era. The online education system handles personal information of teachers and students, information on attendance and evaluation, so security must be considered. In particular, there are many issues to be solved for security problems in the untact education environment, and much discussion has not been made yet. Therefore, more attention is needed for secure untact educational environment[1]. May et al. mentioned that the personal information of participants must be strongly protected as security and personal information protection problems in the remote online education environment are increasing[2]. This study pointed out that users are concerned about the exposure of their personal information, and emphasized the importance of protecting learner data safely. In addition, it emphasized that privacy protection, reliability of resources used for learning, hyper-connected access, protection of privacy for location information, single sign-on-based authentication, and DRM are important elements in the online education system. Luminita et al. emphasized that the online education platform must meet basic security features such as integrity, access control, non-repudiation, and availability, and mentioned vulnerabilities affecting the online education environment[3]. Weippl et al. asserted the importance of CIA (confidentiality, integrity and availability) to maintain security. He also noted that all other requirements can be explained by these three basic attributes[4]. Meghana et al. evaluated the security issues and vulnerabilities of the online education platform, discovered vulnerabilities and flaws in the current e-learning learning environment, and designed a security model for e-learning security[5]. Until now, a lot of research has been conducted on the security risks of online education systems, but the focus is mainly on the research on security in an LMS environment that plays pre-recorded images. In this way, the security problem for real-time untact education, which requires two-way communication, cannot be completely solved. Various components such as teachers, students, content, and evaluation should be considered in the untact education environment, and these components should be securely protected. In this paper, it is possible to prevent the manipulation of attendance and evaluation data in an online education environment by using a changeable blockchain technology, and to solve the privacy protection problem caused by video exposure[6,7,8,9,10].

2. Proposal of new untact education system

2.1. Overview

The method proposed in this article is shown in (Fig. 1). The proposed system consists of an LMS server, a blockchain server, and a client that students can access, and students can access the LMS server through a PC or mobile environment. Teachers and students can learn through the LMS server, and each student has a corresponding blockchain. The blockchain contains student face information, behavior analysis information according to video analysis, access log, and evaluation information. In other words, each blockchain records the learning information of the student in the course of the class, and once saved, it cannot be changed due to the nature of the blockchain. This characteristic is very effective in preventing malicious manipulation of achievement levels in the learning process. In the figure, one block of the blockchain mapped to the student is a conceptual part, and the actual blockchain is stored on the servers that make up the blockchain. The data stored in the blockchain is encrypted, and outsiders cannot illegally decrypt the original data[11].

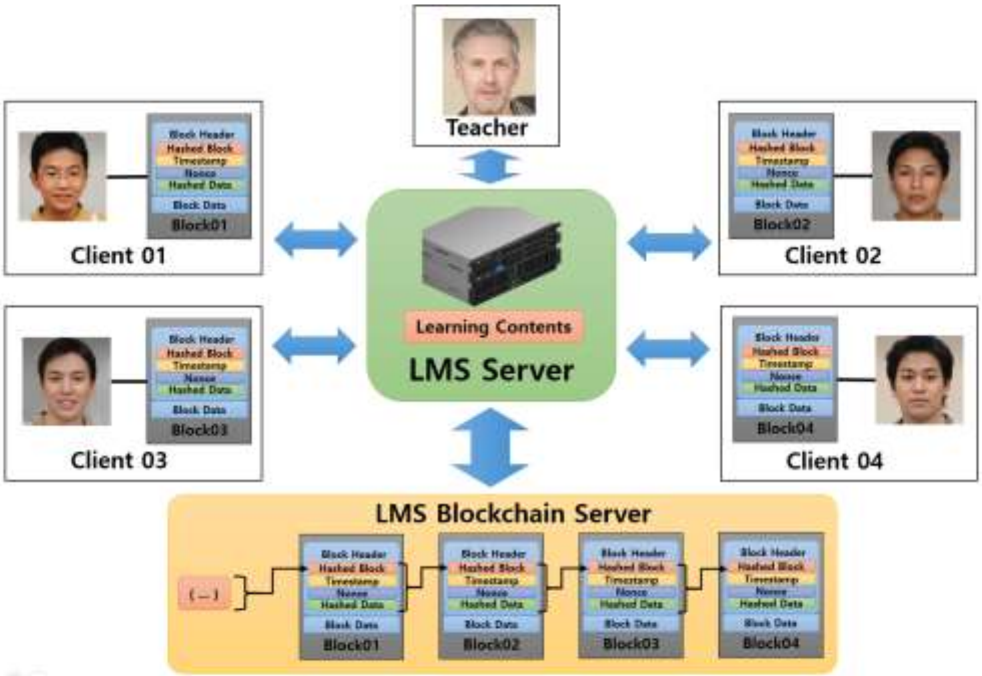

Fig. 1. Overview of the proposed method

2.2. Types of data

The types of learning data stored in the blockchain are shown in Fig. 2. Blockchain data contains the following four types of information.

a) Learner's identity: Learner's identity information is stored for identification, and the data must be encrypted.

b) Masked face data: Do not store the original image data, but save after masking. If the face information is saved as it is, learner's privacy may be exposed. Therefore, for privacy protection, the face image is appropriately masked and stored.

c) Behavior analysis data: Stores the results of behavior analysis in the learning process. Behavior analysis is performed through video analysis, and it is possible to determine inappropriate behavior prevention and learner concentration.

d) Access log: A log of the learner's access to the LMS server (learning start and end) is stored.

e) Test and evaluation data: The result value of the test is stored. Test results are sensitive personal information and must be encrypted and stored, and must not be exposed to outsiders.

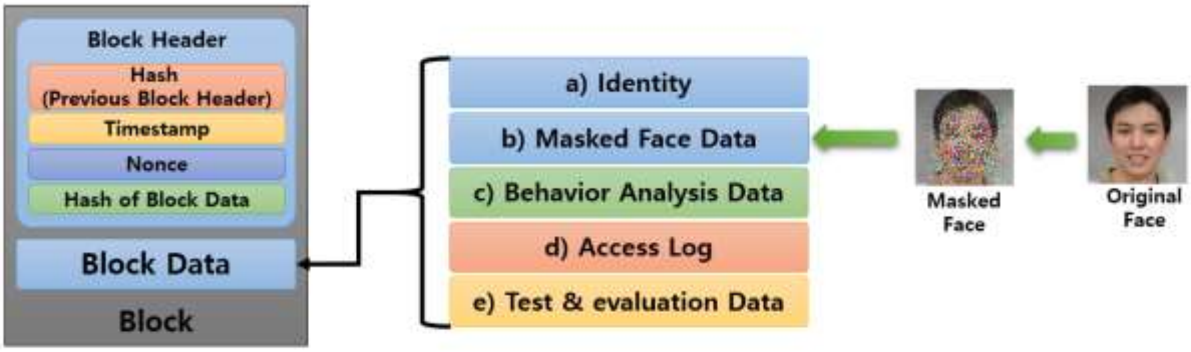

Fig. 2. Types of data stored in the blockchain

3. Procedure of the proposed method

The procedure for storing learning data on the blockchain is shown in Fig. 3. First, user authentication is performed, and when learning begins, the LMS system analyzes learners' behavior. The content of the learner's behavior analysis is delivered to the teacher in real time, and the data is used as data to increase the efficiency of the class. After learning is evaluated, when learning is finished, the teacher approves the end of learning. After that, the learning data is stored in the blockchain, and the learning data cannot be modified and is safely stored in a state that cannot be manipulated.

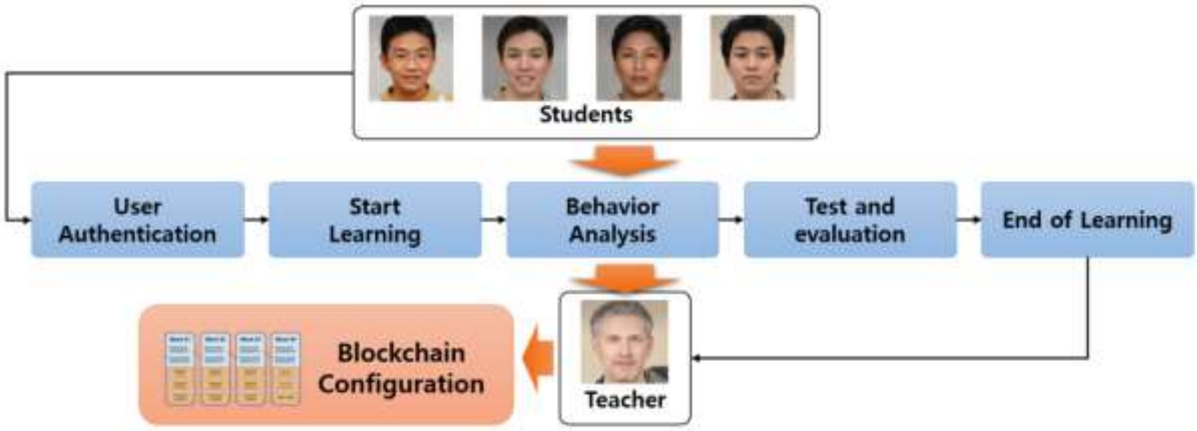

Fig. 3. Procedure of the proposed method

3.1. User authentication and start learning

Before learning begins, it is necessary to check whether the learner is a legitimate user through login. In the proposed method, two factor authentication is performed for user authentication. For authentication, ID/password authentication and face recognition authentication of the user are required. In principle, if face recognition does not work, it is treated as not authenticated. However, if facial recognition information does not exist in advance or if special permission is obtained, authentication is possible with the user's ID. Face recognition information registered in advance is required for face recognition, and such face recognition-based authentication prevents unauthorized access by anyone other than the self. In particular, in the process of taking a test for evaluation, it is necessary to more thoroughly perform face recognition-based authentication.

3.2. Behavior analysis in the learning process

It is difficult to provide a timely educational environment because the existing analysis of learning achievement is mainly focused on post evaluation. For example, it was not easy to judge how much a student concentrates on a class in the existing class. The proposed untact education system can provide a timely educational environment in terms of analyzing such learning achievements in real time. While learning is in progress, students' behavior is identified through video analysis. The degree of concentration of class can be determined through the analysis of student behavior, and this video analysis has the advantage of overcoming visual and verbal barriers. If a student takes an inappropriate action, a warning alarm may occur. And the teacher can check the student's concentration in real time and respond appropriately. If the student's concentration is very low, the teacher can choose an appropriate method to concentrate the students, so that the education can be conducted efficiently.

3.3. Test and evaluation

At the end of the class, you can take the appropriate online test. Student evaluation results are recorded on the blockchain, and malicious manipulation of evaluation results is impossible through this method. Blockchain data is fundamentally impossible to manipulate, so the integrity of the evaluation results can be guaranteed. Evaluation results are sensitive personal information and need to be handled in secret. Therefore, when storing in the blockchain, the evaluation result must be encrypted and stored.

3.4. End of learning and blockchain configuration

The header data of the blockchain is not recorded until the end of the learning, and all blockchain data including all the blockchain headers are stored by the teacher's approval after the entire learning is completed. Blockchain has the characteristic that the hashed value of the header information of the previous block is stored in the next header. Therefore, at the end of learning, through the teacher's approval, the header of each blockchain in which the student's learning information is chained and stored in the blockchain server. After the blockchain is recorded through the teacher's approval, the data on learning cannot be modified, and if modification is needed later, a separate blockchain must be configured and stored.

4. Analysis

The proposed method is analyzed in terms of tampering prevention, learning data protection, illegal use prevention, behavior analysis, and privacy protection.

(1) Tampering prevention: In the proposed method, after learning, all learning data is stored in a blockchain according to the teacher's approval. By applying this blockchain method, it is fundamentally impossible to manipulate data. In particular, illegal manipulation of academic achievement is impossible, and data manipulation is fundamentally impossible because data necessary for follow-up such as access logs are left.

(2) Learning data protection: If learning data is illegally exposed to a person with malicious intent, the personal information of learners may be infringed. As a feature of this paper, blockchain and encryption are used to protect learning data. In particular, because information on test and evaluation data is encrypted and stored, learning data can be safely stored.

(3) Illegal use prevention: In the proposed method, 2-factor authentication is performed. By performing ID/password method and facial image recognition-based authentication, it is not possible to learn normally if it is not the person. If someone other than a legitimate user wants to proceed with learning, it is effective to prevent illegal learning because it is not normally authenticated.

(4) Behavior Analysis: Through image data-based behavior analysis, appropriate actions can be taken when learners take inappropriate actions. Meanwhile, the user's concentration can be checked through behavioral analysis, and this concentration is transmitted to the teacher. The teacher can use the learner's concentration in class and can choose various methods to increase the concentration.

(5) Privacy protection: In the learning process, the learner's face image is collected, and the collection of the face image is an essential factor in determining whether or not a legitimate learner is. Collecting such facial images can be a problem in terms of privacy. In the proposed paper, the user's face collected through facial recognition is masked and stored. Therefore, since the actual face recognition data is not stored, the privacy of the learner can be protected.

5. Conclusion

The importance of information security cannot be overemphasized and is a factor that must be considered according to changes in environment and systems. In particular, there is a situation of concern about exposure to more security threats in the untact education environment than in the existing learning environment. As online access becomes easier, the education system may expose information through various routes, such as hacker attacks or stealing information from insiders. Meanwhile, in the untact educational environment, privacy exposure to learners may occur, and various information such as facial recognition information and test evaluation data may be exposed. With the advent of the COVID-19 environment, the importance of an untact educational environment is growing. Currently, a variety of untact education is being attempted, but there are not many security studies on untact education. However, the untact environment can be vulnerable to security and various cyber attacks can occur, so safe countermeasures are essential. In this paper, we proposed a safe untact education system using blockchain. The proposed method stores facial masking images, learner behavior analysis data, access logs, and test and evaluation information in the blockchain. Blockchain itself has strong integrity, and as learning data is stored in the blockchain, artificial manipulation by hackers is impossible. In addition, as an advantage of the proposed method, timely education is possible because it is possible to identify learners' concentration through real-time behavior analysis and accompany appropriate measures from teachers. In addition, if learners take inappropriate actions, appropriate warning measures can be taken, which helps smooth untact learning. The COVID-19 outbreak will further accelerate the untact education environment. In order to protect learners' privacy and achieve efficient education, many studies on the untact education system will need to be conducted in the future.

Acknowledgements

This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea(NRF-2019S1A5C2A04083374). And, this work was supported by the Korea Foundation for the Advancement of Science and Creativity(KOFAC) grant funded by the Korea government(MOE).

References

[1] Jeghal, A., Oughdir, L., and Tairi, H. (2016). "Politic of security, privacy and transparency in human learning systems," Education and Information Technologies 21(3), 521-530.

[2] May, M., and George, S. (2011). "Privacy Concerns in E-learning: Is UsingTracking System a Threat?," International Journal of Information and Education Technology 1(1), 1-8.

[3] Luminita, D. C. (2011). "Information security in E-learning Platforms," Procedia-Social and Behavioral Sciences 15, 2689-2693.

[4] Weippl, E. R., and Ebner, M. (2008) Security privacy challenges in e-learning 2.0, In E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education. Association for the Advancement of Computing in Education (AACE), Las Vegas, U.S.A., 4001-4007.

[5] Bhatia, M., and Maitra, J. K. (2018) E-learning Platforms Security Issues and Vulnerability Analysis. In 2018 International Conference on Computational and Characterization Techniques in Engineering & Sciences (CCTES). IEEE, Lucknow, India, 276-285.

[6] Park, N., Kwak, J., Kim, S., Won, D., and Kim, H. (2006) WIPI mobile platform with secure service for mobile RFID network environment, In Asia-Pacific Web Conference, Springer, Berlin, Heidelberg. 741-748.

[7] Park, N., and Kim, M. (2014) "Implementation of load management application system using smart grid privacy policy in energy management service environment," Cluster Computing 17(3), 653-664.

[8] Lee, D., and Park, N. (2017) "Geocasting-based synchronization of Almanac on the maritime cloud for distributed smart surveillance," The Journal of Supercomputing 73(3), 1103-1118.

[9] Park, N., and Kang, N. (2016) "Mutual authentication scheme in secure internet of things technology for comfortable lifestyle" Sensors 16(1), 20.

[10] Kim, J., Park, N., Kim, G., and Jin, S. (2019) "CCTV Video Processing Metadata Security Scheme Using Character Order Preserving-Transformation in the Emerging Multimedia" Electronics 8(4), 412.

[11] Lee, D., Park, N., Kim, G., and Jin, S. (2018) "De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment" Peer-to-Peer Networking and Applications 11(6), 1299-1308.