Journal of the Korea Convergence Society
Vol. 11. No. 3, pp. 27-35, 2020

ISSN 2233-4890 / eISSN 2713-6353
https://doi.org/10.15207/JKCS.2020.11.3.027

교육행정정보시스템 학교생활기록부 데이터의 안정성 확보를 위한 블록체인 설계 및 구현

김희경[1], 박남제[2*]
[1]제주대학교 일반대학원 융합정보보안학협동과정 석사과정
[2]제주대학교 교육대학 초등컴퓨터교육전공 교수

Design and Implementation of Blockchain for Securing Data of National Education Information System School Life Records

Heekyung Kim[1], Namje Park[2*]
[1]Master's Course, Department of Convergence information Security, Graduate School, Jeju National University
[2]Professor, Department of Computer Education, Teachers College, Jeju National University

요 약 본 연구의 목적은 시·도교육청 교육행정정보시스템 학생생활기록부가 중요한 교육활동의 기록이나, 지속적으로 불법유출·조작하는 등의 문제점을 방지하기 위한 기술적 구현방법을 연구하는 것이다. 이를 위해 본 논문에서는 정해진 조직 또는 개인만이 참여할 수 있는 프라이빗 블록체인을 적용함으로서 외부자에 의한 블록네트워크 참여를 방지하고, 생활기록부 학생정보 블록과 접근기록 블록 두 종류의 블록 데이터를 생성하여 정당한 권한을 부여받은 실무자에 의해서만 등록, 수정, 접근할 수 있는 블록 메커니즘을 제시하였다. 그 결과, 제3자에 의한 생활기록부의 위·변조방지와 생활기록부의 무결성 확보를 할 수 있는 하나의 대안을 마련하였으며, 실제 교육행정정보시스템에 적용하게 된다면 생활기록부 운영과 관리가 신뢰할 수 있다는 사회적 공감대를 확보하게 될 것이다.

주제어 : 학교 생활기록, 학생기록 블록, 접근데이터 블록, 프라이빗 블록체인, 데이터 암호화

Abstract The purpose of this study is to study the technical implementation methods to prevent problems such as the record of important educational activities of the student life record department or the continuous illegal leakage and manipulation. To this end, in this paper, by applying a private blockchain that can be participated only by a given organization or individual, it prevents outsiders from participating in the block network, and creates legitimate authority by creating two types of block data: student information block and access record block in the life record book. We proposed a block mechanism that can be registered, modified, and accessed only by authorized staff members. As a result, we have prepared an alternative to prevent forgery and alteration of the living records by third parties and to secure the integrity of the living records. If applied to the educational administrative information system, social consensus will be established that the operation and management of the life record book is reliable.

Key Words : School Life Records, Student Record Block, Access Data Blcok, Private BlockChain, Data Encyption

*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 Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) [2019-0-00203, The Development of Predictive Visual Security Technology for Preemptive Threat Response].
*Corresponding Author : Namje Park(namjepark@jejunu.ac.kr)
Received January 29, 2020 Revised February 27, 2020
Accepted March 20, 2020 Published March 28, 2020

1. 서론

전국 초·중등 교육과 행정업무를 전자적으로 구현한 교육행정정보시스템(National Education Information System, NEIS(나이스))은 2000년대에 처음 구축되어, 2011년도에 2차 전면개편에 이어 2022년에 다양한 교육정책 지원과 노후 장비 교체, IT신기술 발전에 따른 사용자 편의성 향상을 위하여 3차 전면 개편될 예정이다[1,2].

교육부와 17개 시도교육청 협의체에서 2018년 8월부터 전면개편을 위한 ISP 추진 중이며, 안정성이 확보된 시스템 개편을 위하여 정보기술환경 변화와 웹표준에 대처할 수 있도록 정보기술 요소를 분석하여 적용할 수 분야를 연구 중에 있다. 그 중에서 정보보안을 위한 블록체인기술 적용방향에 대해서도 검토 중이다[3-5].

교육행정정보시스템은 교무학사, 인사, 회계 등 전 교육행정업무 총 43개 단위업무, 265개 세부업무로 구성되어 있으며, 그 중 교무업무의 핵심인 학교생활기록은 대학입시 전형에서 중요한 부분이며, 중요한 만큼 무단 학생부 정정 및 성적 조작, 열람, 유출 하는 등의 사건이 발생하기도 한다[6,7]. 이러한 위험성을 방지하고 데이터의 안정적인 보존을 위하여 생활기록부 접근 시 사용자 2차 인증, 수정이력 보관, 권한부여 강화 등의 방안을 적용하고 있기도 하나, 악의적이고 조직적으로 조작을 할 수 없게 하기 위한 시스템 구현이 필요한 시점이다.

인터넷이 정보를 교환하는 기술 혁명이였다면 블록체인은 신뢰를 기반으로 한 가치를 교환할 수 있는 P2P(Peer-To-Peer) 기반의 분산시스템이다. 탈중앙화와 데이터 무결성 유지가 특색인 블록체인의 핵심기술은 P2P네트워크, 암호화, 분산장부, 분산합의와 같이 크게 4가지 기반기술로 구성되어 있다[8,9].

본 논문에서는 정해진 조직 또는 개인만이 참여할 수 있는 프라이빗 블록체인을 적용함으로서 외부자에 의한 블록네트워크 참여를 방지하고, 교육행정정보시스템의 정당한 관리자가 아닌 제 3자에 의한 생활기록부의 위·변조방지와 생활기록부의 무결성 확보를 위한 하나의 대안을 제안한다.

2. 관련 연구

2.1 교육행정정보시스템

교육행정정보시스템은 2000년 전자정부 구현의 일환으로 대한민국의 초·중등 교육과 관련하여, 1만여 개 학교와 181개 지역 교육지원청, 17개 시·도 교육청, 교육부를 인터넷으로 연결하여 교무학사, 인사, 회계 등 전 교육행정업무를 전자적으로 연계 처리할 수 있도록 함으로써 교육행정의 효율성과 대국민 서비스를 향상하기 위해 구축된 정보시스템으로 시도교육청별로 시스템을 구축하여 서비스를 운영하고 있으며, 교직원 약 55만명, 학생·학부모 약 700만 명 사용자가 사용 중이다[10].

교육행정정보시스템 주요 운영 현황은 '초·중등 업무지원'으로 4개시스템, 43개 단위업무, 265개 세부업무로 운영되고 있으며, '대국민서비스'는 학생 46종, 학부모 59종, 홈에듀민원 18종을 제공하고 있다. Table 1은 교육행정정보시스템에서 진행되고 있는 전반적인 운영 업무에 대해 보이는 것이다.

Table 1. Overall operation of National Education Information System

['18.3]

	General Administration	School Affairs	School administration	Public Service
Main Task	HR, salary, complaints, and lifelong education	Academic Affairs / Bachelor, Admission, Health,etc.	Scholarship, after school physical education, lunch	Public Service, Survey, etc.
Task Scale	21 unit tasks, 102 subtasks	7 unit tasks, 92 subtasks	11 unit tasks, 55 subtasks	4 unit tasks, 16 subtasks

일반행정, 교무업무, 학교행정, 대국민서비스 4개 시스템 중에서 학생 정보가 들어간 주요시스템인 '교무업무'는 7개 단위업무, 92개 세부업무로 구성되었으며 교무학사 단위업무 안에 학교생활기록부가 있다[11].

Fig. 1과 같이 교육행정정보시스템에는 다양한 내용이 기록되며, 기록에 대한 신뢰성을 보장해야만 한다. 학교생활기록부의 신뢰성 붕괴는 학생에 대한 보장이 불가하게 될 수 있으며, 이는 곧 형평성에 어긋나는 결과를 보일 수 있다.

2.2 학교생활기록부

교육행정정보시스템 안에서도 교무업무의 핵심인 학교생활기록은 초중등교육법 제25조에 따라 학교의 장이 학생의 학업성취도 및 인성 등을 종합적으로 관찰·평가하여 학생지도 및 상급학교(대학 포함)의 학생 선발에 활용할 수 있는 학생의 인적사항, 학적사항, 출결상황, 자격증 및 인증 취득상황, 교과학습발달상황, 행동특성 및 종합의견 등을 작성하고 관리하도록 하고 있다. 매년 학교생활기록부 대입전형자료를 대학에 온라인으로 제공하여

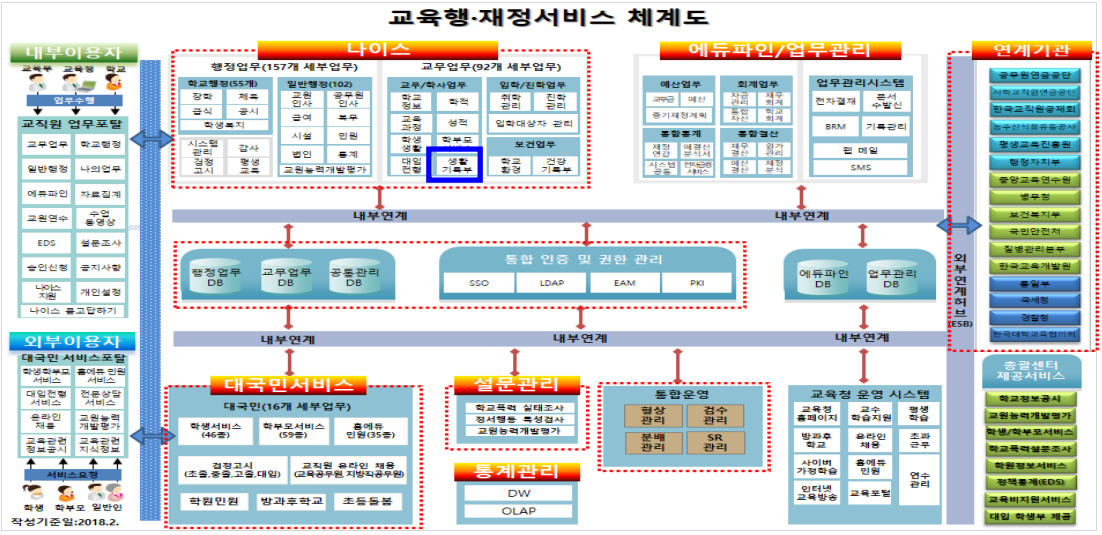

Fig. 1. Educational Administration Financial Service System

대학입학 당락의 조건이 되기도 한다.

Table 2와 같이 학교업무영역에서 이런 중요한 학교생활기록부의 부당 정정을 예방하고 공정성 제고를 위하여 학교생활기록부관련 사용자 접근권한 부여시 학교장이 결재하고 있으며, 최초 입력·저장할 때에는 사용자 2차 인증(ARS[1], mOTP[2])을 하게하여 본인인증 절차를 강화하고, 학교생활기록부 정성적 기재영역[3]에 대한 수정이력은 보관하는 등 안전장치를 마련하여 운영을 강화하고 있다[12,13].

법률적으로는 초·중등교육법 제30조의6에서 학생생활기록부는 해당 학생(학생이 미성년자인 경우에는 학생과 학생의 부모 등 보호자)의 동의없이 제3자에게 제공하여서는 안 되도록 규정하고 있으며, 자료는 준영구로 보존하며 학생 졸업 후 5년동안 학교에서 보관하고, 이후에는 공공기록물관리에 관한 법률 시행령에 따라 보존·관리한다.

1) ARS(automatic response system) : 음성으로 된 각종 정보를 자동으로 전달하는 시스템

2) mOTP(mobile one time password) : 휴대전화나 스마트폰 등 이동단말에서 사용하는 1회용 비밀번호

3) 정성적 기재영역 : 교과학습발당상황(세부능력 및 특기사항, 특기사항), 창의적 체험활동 상황, 진로 희망사항(희망사유), 자유학기활동상황. 행동특성 및 종합의견

Table 2. School Affairs Area

Unit Work	Main Function
Academic Affairs / Bachelor	-Management support, school information, curriculum, school records, student life, grades, school life records, individualized education management
Admission / Academic	-Entering elementary school, entering middle school, entering high school
Health	-Health records, infectious patients management, health examination, statistical management
Academic Affairs / Bachelor (Overseas Korean School)	-School information, curriculum, school records, student life, grades, school life records
Academic Affairs / Bachelor (Gifted school)	-School information, curriculum, school records, student life, grades, school life records
Career map	-Career related matters management, career related matters transmission
Student Preservation	-Student Preservation (Elementary, Middle, High, Special, School District)

자료의 정정은 학교의 매 학년이 종료된 이후에는 당해 학년도 이전의 학교생활기록부 입력자료에 대한 정정은 원칙적으로 금지하고 있으나, 객관적인 증빙자료가 있는 경우에는 학교 학업성적관리위원회의 심의 절차를 거친 후 결재 절차에 따라 정정할 수 있다.

2.3 교육행정정보시스템 보안 아키텍쳐

교육행정정보시스템에서의 보안구성은 사용자 PC보안에서 데이터 암호화보안까지 Table 3과 같이 7단계로 구성하고 있다[14].

Table 3. Step 7 Configure Security

Phase	Contents
1	Personal PC firewall, antivirus, keyboard security, patch management system, DRM
2	Service access control through user authentication
3	Access control to the network
4	Harmful detection and blocking of networks and servers
5	Secured stability of network communication between user PC and server
6	Server security (access control, authority control, audit data generation, account management, etc.)
7	Protection measures for stored data (encryption, access control, audit data generation, account management, etc.)

Fig. 2와 Fig. 3과 같이 교육행정정보시스템 시스템 보안 영역은 통제(접근제어, 인증), 탐지(웹쉘탐지, 웹DRM, 백신), 암호화(표준 보안 API, DB 암호화 등), 관리(로그수집, 취약점 관리 등) 4가지 영역으로 구분하며 이에 대응하는 솔루션을 설치하여 보안 관리를 하고 있다.

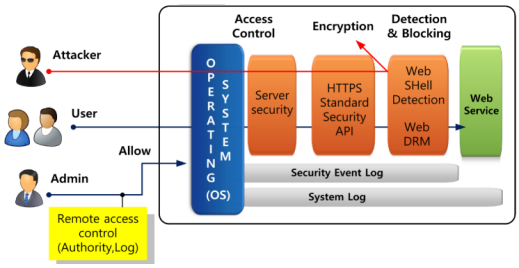

Fig. 2. System security zones

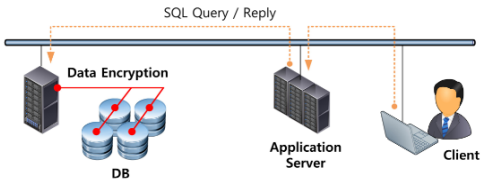

Fig. 3. Data Encryption

2.4 블록체인 기술

블록체인은 전송하고자 하는 데이터를 '블록'이라고 하는 용기에 암호화 처리하여 담고, 이 블록을 P2P방식으로 상대에게 직접 전송하거나 수신하는 컴퓨터 통신기술을 말하며, 이러한 송수신 내역이 네트워크에 참여한 모든 이용자들의 컴퓨터에 분산하여 저장된다. 블록체인의 핵심가치는 조작 불가능하고 안전한 기록의 공동(분산)관리에 있으며, 다양한 기술적 보장을 기반으로 투명성과 신뢰성을 높이는 기술이다. 블록체인의 특징은 아래의 Table 4와 같다.

Table 4. Blockchain Features

Characteristic	Contents
Decentralized	Participants create and manage activities such as verification, approval and agreement
Transparency	Blocks are created and sent to all participants at the same time, shared so that all participant s are watched
Immutability	For data modulation, the hash value of all the blocks created after this block must be recomp uted and recorded in more than half of user's blocks.
Availability	A distributed system blockchain is not interrupt ed by a node failure.

블록체인은 2008년 익명의 '사토시 나카모토'가 연구 공개한 이후 1세대(2009~2014년, 암호화폐 분야), 2세대(2015년~현재, 스마트 컨트랙트)로 이어지고 있으며, 앞으로 3세대(미래)에는 사회 전반에 블록체인이 적용될 것으로 예측하고 있다[15,16].

Table 5와 같이 블록체인은 접근성 제한 유무에 퍼블릭(Public) 블록체인과 프라이빗(Private) 블록체인으로 나누며, 퍼블릭 블록체인은 누구나 참여 가능하여 거래 내역을 볼 수 있어 높은 보안성과 투명성을 보장하지만, 개인의 금융 정보나 중요 데이터가 네트워크상으로 오고 갈 수 있기 때문에 적합하지 않을 수 있다. 이 점을 보완해 줄 수 있는 프라이빗 블록체인은 거래 내역을 볼 수 있는 권한을 받은 사람만 열람이 가능한 장점을 가지고 있다[17-21].

Table 5. Public vs. Private Blockchain Comparison

Division	Public	Private
Accessibility	Everyone	Authorized person
Speed	Slow(7-20TPS)	Fast(1,000TPS+)
Identity	Anonymous node	Identified Node
Fees	Necessary	Not necessary or almost
Hard fork	Possible	impossible
Upgrade	Difficulty	facility
Decentralized	Height	lowness
Consensus Algorithm	PoW, PoS, etc.	BFT series
Representative cryptocurrency	Bitcoin, Ethereum, etc.	Ripple, icon, etc.

3. 제안된 블록체인 기반 안전한 생활기록부 데이터 보호방안

3.1 생활기록부 작성 및 관리 사항

학교에서는 학교생활기록 작성 및 관리지침(교육부 훈령)을 준수하여 학생의 학교생활기록을 작성 및 관리하며, 그 기재 내용은 Table 6과 같다.

Table 6. Description of School Life Records

Division	Contents
Personal Information	Student's name, resident registration number and address
Pharmacy	The name of the graduated school, the date of graduation, and any change in school attendance before enrolling
Attendance Status	Student Attendance Status by Grade
Status of certification and certification	Name, number, date of acquisition and type of issuer and certification, content, date and year of certification
Development of Teaching and Learning	Coursework, course names, evaluation results, and progress of learning activities
Behavioral Characteristics and Overall Opinion	Opinion for comprehensive understanding of students 'behavioral characteristics and students' completion of school education
School Information	The grade, class, number, and name of the homeroom teacher
Awards	Name, grade, rank, award period and awarding organization
Creative experience	Voluntary, volunteer, club, and career activities conducted while at school
Reading activity	Title and author of the book the student reads while completing the middle or high school curriculum
Free Semester Activities	Results of free semester activities conducted by students during the free semester

3.2 블록체인 기반 생활기록부 보호기법

제안하는 블록체인 기반의 생활기록부 데이터 보호 기법은 기존의 일반적인 RDB(Relation Database)에 학생의 생활기록부 기록을 암호화하여 저장하여 관리하는 기법에 대해 블록체인을 적용함으로서 생활기록 데이터에 대한 무결성을 보장하고, 데이터의 위·변조를 방지함을 목적으로 한다. 제안된 메커니즘은 프라이빗 블록체인을 적용하며, 생성되는 블록은 학생의 생활기록부에 대한 정보를 가지는 학생 정보 블록과 학생정보에 접근하는 사용자의 정보를 기록하는 접근기록 블록의 두 종류의 블록 데이터를 생성한다. Fig. 4는 생성되는 블록을 가시적으로 보이는 것이다[22-30].

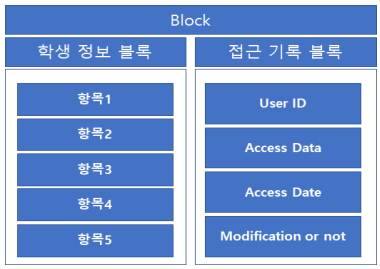

Fig. 4. Proposed block structure

본 논문에서 제안하는 메커니즘은 학교에서 작성된 생활기록부의 기록을 교육행정정보시스템의 서버에 등록하게 되면, 등록된 기록은 암호화된 데이터로서 블록네트워크에 기록된다. 블록 네트워크에 암호화되어 기록되어 있는 생활기록부 정보는 정당한 사용자에 의해 요청될 수 있으며, 사용자의 요청이 들어오면 암호화된 생활기록부

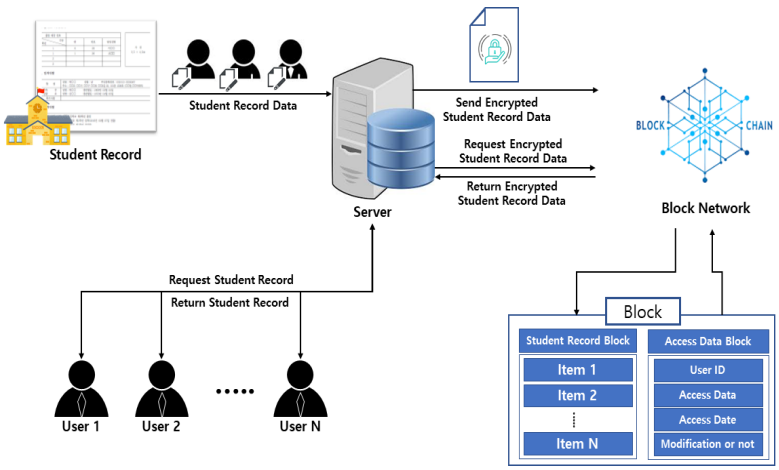

Fig. 5. Blockchain-based Life Records Data Protection Mechanism

를 사용자에게 전송하고, 사용자가 제공된 생활기록부에 대한 이용이 종료되면, 접근기록 블록을 생성하고 수정된 생활기록부에 대한 블록을 생성한다. Fig. 5는 메커니즘의 전반적인 구성도를 보이는 것이다.

3.3 블록체인 기반 생활기록부 데이터 등록·접근통제

제안된 블록체인 기반의 생활기록부 데이터 보호 메커니즘은 기존의 RDB를 이용하여 기록되었던 생활기록부에 대한 신뢰성을 강화하기 위해 제안하는 내용으로 사용자 등록, 학생정보 등록, 학생정보 열람 및 수정의 3개로 구성되며, 해당 내용을 블록체인을 이용함으로서 기록에 대한 위변조를 방지하고, 학생기록부의 신뢰성 향상을 목적으로 한다[31-36].

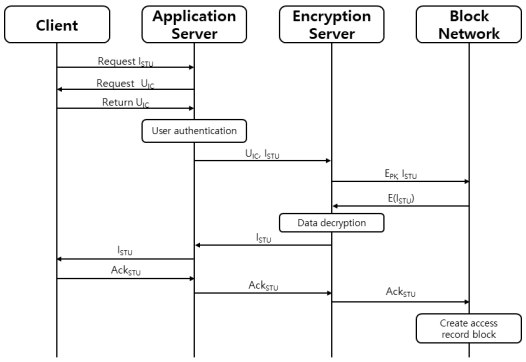

Fig. 6. Blockchain-based Life Records Student Information View and Correction Process

사용자 등록 과정은 관리자, 실무자(학생기록의 생성 및 수정 담당자), 열람자의 세 가지 역할로 구분하며, 관리자는 모든 기록에 대한 읽기의 권한을 가진다. 실무자는 자신의 식별코드를 사용하여 등록한 학생기록에 대한 읽기, 쓰기, 삭제의 권한을 부여한다. 열람자는 학생 본인 또는 학생의 학부모에 부여되는 권한으로 본인의 기록에 대한 읽기 권한만을 제공한다. 이와 같은 사용자의 접근권한은 Application Server에 기록된다. Application Server는 사용자에 대한 식별정보와 식별코드, 접근권한을 기록하며 사용자에 대한 인증과 접근제어를 수행한다.

학생정보 등록 과정은 실무자에 의해서만 이뤄질 수 있으며, 인증된 사용자가 학생정보의 등록을 Application Server에 요청하면 Application Server는 요청된 데이터를 Encryption Server로 전송하고, 전송된 데이터는 공개키 암호화를 기반한 공개키에 의해 암호화된다. 암호화된 데이터는 블록 네트워크에 기록된다.

마지막으로 학생정보 열람 및 수정 과정은 Fig. 6을 통하여 그 과정을 보이고 있다. 그림에서 사용된 용어는 Table 7과 같다.

Table 7. Abbreviation

Abbreviation	Contents
ISTU	Student Information
UIC	User Identification Code
EPK()	Encryption Public Key
E()	Encrypted Data
AckSTU	Data Acknowledgement

사용자에 의해 학생기록 접근 요청이 인가되면, Application Server는 사용자로부터 식별코드를 받아 사용자를 인증하고, 요청한 데이터와 사용자 식별코드를 Encryption Server로 전송한다. Encryption Server에서는 요청한 데이터를 식별정보에 대한 공개키와 같이 Block Network로 전송하고, Block Network에서는 데이터를 반환한다. 반환된 데이터는 서버를 거쳐 사용자에 전송되며, 사용자의 데이터 접근이 확인되면, 사용자 접근 블록을 생성한다.

4. 구현

본 장은 제안된 메커니즘의 Application Server와 Encryption Server의 DB에 대한 간략한 구현과 Block Network에 기록된 내용을 보이도록 한다. Fig. 7은 각각 Application Server와 Encryption Server의 내용을 보이는 것이다.

No	User ID	User IC	User AC
1	A	AD20190101F1	w,r,e
2	B	AD20190101E5	w
3	C	AD20190101C8	w

User IC	User PK
AD20190101F1	0x1E9327AC12D52123AD
AD20190101E5	0x2E9412BB12D1219389
AD20190101C8	0x7E9742EE12B1219AD4

Fig. 7. Application Server(top) and Encryption Server (bottom)

Fig. 7에서 User Id는 교육행정정보시스템에 접근하는 사용자 식별자이며, User IC는 사용자 식별자에 매칭되는 사용자 식별코드이며, User PK는 사용자 식별코드에 매칭되는 사용자 식별키로 암호화하기 위한 공개키를 의미한다. Encryption Server에서 사용자에 대한

비밀키에 의해 암호화된 학생기록 정보는 Block Network에 기록되며, 학생기록을 가지는 블록은 Fig. 8과 같이 생성되게 된다. Fig. 8은 내용의 일부를 시각화하기 위하여 임의로 제작하였으며, 실제 교육행정정보시스템에 구현하게 되면 학생생활기록부의 학생데이터를 블록 네트워크에 기록 작성하게 된다. 학생데이터 기록의 블록 네트워크 암호화를 통한 제 3자에 의한 유출을 방지할 수 있고 무결성 유지를 기대할 수 있다.

Fig. 8. Block data(top) and Data recovery(bottom)

Fig. 8에서 상단 그림은 이더리움 오픈소스 구조체로 임의로 구현한 것이며, 입력한 값에 대한 블록데이터이다. 하단 그림은 블록데이터를 복호화 했을 때의 테스트 데이터이다. 즉, ABC라는 학생의 생활기록부 개인정보의 6개 항목을 임의의 블록데이터로 구현한 것이다.

실제 교육행정정보시스템에서 생활기록부영역에 대한 무결성 확보를 위하여 블록데이터를 구현한다면 인적사항, 학적사항, 출결상황, 교과학습발달상황, 수상경력 등 입시정보에 기초가 되는 여러 중요 항목을 적용하는 것이 바람직하다.

본 논문에서는 정해진 조직 또는 개인만이 참여할 수 있는 프라이빗 블록체인을 적용함으로써 외부자에 의한 블록 네트워크 참여를 방지하고, 생활기록부 학생정보 블록과 접근기록 블록 두 종류의 블록 데이터를 생성하여 정당한 권한을 부여받은 실무자에 의해서만 등록, 수정, 접근할 수 있는 블록 메커니즘으로 제3자에 의한 생활기록부의 위·변조방지와 생활기록부의 무결성 확보를 위한 하나의 대안을 제안한 것으로써, 2022년 3차 교육행정정보시스템 전면개편에 적용하게 된다면 생활기록부 운영과 관리가 안정적이고 신뢰할 수 있다는 사회적 공감대를 확보하게 될 것이다.

5. 결론

17개 시도교육청이 2015년부터 2018년까지 진행한 학교 감사결과 시험지 유출이 숙명여고를 포함해 모두 13곳으로 드러났으며, 학교생활기록부 부적정 기재하여 적발된 중고교도 15곳으로 나타났다. 2015년에는 경기 분당 대진고에서 교무부장이 딸의 학생부를 조작했다가 파면된 사례도 있었다. 최근에는 모 법무부장관 후보 딸의 생활기록부가 본인의 동의없이 유출되어 정치권의 이슈로 사용되는 등 교사와 학생에 대한 교육권과 인권을 침해하는 사건도 발생하고 있다. 이렇듯 교육행정정보시스템 안에서 학생생활기록부는 학생의 학교생활 전반의 교육활동과 함께 개인의 성장과정이 매우 세밀하게 기록되어 있는 중요한 개인정보이며 교육활동 결과물이므로 이 데이터에 대한 불법유출과 위·변조를 방지하여 무결성을 확보할 수 있어야 한다.

위와 같은 문제를 보완하기 위해서 본 논문에서는 프라이빗 블록체인을 적용하여 외부자에 의한 블록네트워크 참여를 방지하고, 교육행정정보시스템의 정당한 관리자가 아닌 제 3자에 의한 생활기록부의 위·변조방지와 생활기록부의 무결성 확보를 위한 하나의 대안을 제안하였다. 교육행정정보시스템 서버에 등록된 학교생활기록부 데이터는 암호화된 블록네트워크에 기록되며, 정당한 사용자에 의해 요청될 수 있도록 접근기록 블록을 생성하여 수정된 생활기록부에 대한 블록을 생성하여 보호하는 메커니즘이다.

사용자 등록은 관리자, 실무자, 열람자 세 가지 역할로 구분하여 인증과 접근을 통제하며, 학생정보 등록과정은 실무자에 의해서만 등록하여 공개키에 의해 암호화되며 암호화된 데이터는 블록네트워크에 기록된다. 열람 및 수정과정은 요청한 데이터를 인가된 식별정보에 대한 공개키와 같이 Block Network로 전송하고, Block Network에서는 데이터를 반환하며, 반환된 데이터는 서버를 거쳐 사용자에 전송되어 사용자의 데이터 접근이 확인되면 사용자 접근 블록을 생성함으로서 데이터무결성 유지와 사용자 접근통제로 위·변조를 방지할 수 있는 방안을 제안하였다.

그러나 본 논문은 4개 시스템, 43개 단위업무, 265개 세부업무로 운영되는 방대한 교육행정정보시스템이라는 단일시스템에서 그 중 생활기록부라는 하나의 세부업무에 대하여 블록체인기술을 적용하는 실제로 구현해본 연구가 아닌 이론적 연구에 불과하다는 제한점을 가진다.

본 논문의 결과를 토대로 실제 구현할 수 있는 방안이

도출되도록 후속연구를 위한 제언을 하면 다음과 같다.

첫째, 임의의 블록데이터를 구현할 때, 단순히 ABC라는 학생의 생활기록부 6개 항목으로 하였으나, 실제 생활기록부는 7개 분야에 100여개의 항목으로 구성되어 있으므로 모든 항목을 블록데이터로 구현할 필요성이 있는지와 블록크기와 시스템 속도 등의 기술적 측면에서의 구현가능성을 연구할 필요성이 있다. 둘째, 본 연구에서는 Application Server와 Encryption Server를 통한 데이터 기록을 구현하였으나 이 과정조차도 스마트 컨트랙트로 구현할 수 있는 방안이 연구된다면, 데이터 기록과 접근통제, 위변조방지의 모든 과정을 블록체인으로 구현하는 확장된 연구가 될 것이다. 셋째, 생활기록부는 학생졸업후 5년이 지나면 공공기록물관리에 관한 법률 시행령에 의해 기록물로 보존하도록 하고 있으며, 기록물보존관점에서 진본성유지를 위한 블록체인 기술구현 방안 연구도 검토할 필요가 있겠다. 더불어 학생생활기록부이외에 교육행정정보시스템 다른 분야에 블록체인 기반을 확대적용하는 방안 연구와학교에서 off-line상 시험지 유출사고를 방지하기 위해서 블록체인 기반 온라인 학습 평가시스템을 도입하여 투명성 있는 평가와 시험문제 유출방지에 대한 연구도 필요할 것이다.

REFERENCES

[1] D. Y. Lee, J. W. Park, J. H. Lee, S. R. Lee & S. Y. Park. (2017). Blockchain Core Technology and Domestic and Foreign Trends. *Communications of KIISE, 35(6),* 22-28.

[2] J. B. Lee, J. C. Jeong & G. N. Lee. (2013). Current Status and Directions on Writing, Management, and Use of Career Related Records in Transcript of School Record. *Journal of The Korean Society for Agricultural Education and Human Resource Development, 45(4),* 23-52.

[3] H. M. Hong & S. S. Go. (2015). A Study on the Improvement of High School Grade Report and Form of School Life Records. *Journal of the Korean School Mathematics Society, 18(4),* 87-409.

[4] J. Kim, N. Park, G. Kim & S. Jin. (2019). CCTV video processing metadata security scheme using character order preserving transformation in the emerging multimedia. *Electronics, 8(4),* 412.

[5] W. H. Jang & M. J. Kim. (2019). Analysis on elementary school first grade teachers' perception and needs on theme-based integrated curriculum through focus group interview : Focusing on continuity between kindergarten and elementary school. *Journal of Korea Open Association for Early Childhood Education, 24(1),* 509-533.

[6] H. C. Joo, K. S. Hong & J. H. Baeck. (2019). Establishing a Strategy to Develop Online Career Administration System for Korean Student-Athletes through Analyzing Domestic and Foreign Cases. *Journal of Physical Education Humanities and Social Sciences, 58(3),* 159-173.

[7] H. G. Moon & S. H. Cha. (2019). Exploring the Implementation Process of Homeroom-Teacher Administrative Workload Zeroing Policy. *Journal of Education & Culture, 25(2),* 203-225.

[8] D. Lee, N. Park, G. Kim. & S. Jin. (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.

[9] J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira & A. Akutsu. (2015). *The Blockchain-Based Digital Content Distribution System.* Conference of 2015 IEEE Fifth International Conference on Big Data and Cloud Computing, (pp. 187-190). IEEE.

[10] M. W. Lyu & M. G. Park. (2017). A Study on the Methods of Fault Analysis for Security Improvement of National Education Information System(NEIS). *Journal of Multimedia, 20(12),* 1970-1979.

[11] Y. S. Chang & J. H. Cho. (2017). Design and Implementation of Information System Based on Educational Data. *Journal of the Korea Contents Association, 17(6),* 436-451.

[12] N. Park & H. Bang. (2016). Mobile middleware platform for secure vessel traffic system in IoT service environment. *Security and Communication Networks, 9(6),* 500-512.

[13] J. M. Choi & D. Y. Kim. (2017). A Study on Security Management Methods for Information System of Educational Institutions. *Journal of Korean Association of Computer Education, 20(6),* 95-104.

[14] J. Kim & N. Park. (2019). Development of a board game-based gamification learning model for training on the principles of artificial intelligence learning in elementary courses. *Journal of The Korean Association of Information Education, 23(3),* 229-235.

[15] J. Kim & N. Park. (2019). BlockChain Technology Core Principle Education of Elementary School Student Using Gamification. *Journal of The Korean Association of Information Education, 23(2),* 141-148.

[16] Y. A. Park, J. H. Kim & I. K. Kim. (2018). A Case Study on the Application of Ethereum-Blockchain Technology for Electronic Voting System. *Journal of Information Technology and Architecture, 15(2),* 201-218.

[17] D. Lee & N. Park. (2017). Proposal of Technology and Policy Post-Security Management Framework for Secure IoT Environment. *Journal of Korean Institute of Information Technology, 15(4),* 127-138.

[18] S. L. Kim. (2018). Smart Contract System by Blockchain of Real Estate Transaction. *Journal of Real estate law review, 22(3),* 93-124.

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

[20] Y. Jung, W. Jung, S. Oh, D. Lee & N. Park. (2019). AES-GCTR Mode-based Efficient Hybrid Encryption Scheme in Cloud-CCTV Service Environment. *International Journal of Recent Technology and Engineering, 8(Issue-2S6),* 405-408.

[21] D. Lee & N. Park. (2018). Electronic Identity Information Hiding Methods Using a Secret Sharing Scheme in Multimedia-centric Internet of Things Environment. *Personal and Ubiquitous Computing, 22(1) Issue 1,* 3-10.

[22] N. Park, B. G. Kim & J. S. Kim. (2019). A Mechanism of Masking Identification Information Regarding Moving Objects Recorded on Visual Surveillance Systems by Differentially Implementing Access Permission. *Electronics, 8(7),* 735.

[23] N. Park, H. Hu & Q. Jin. (2016). Security and Privacy Mechanisms for Sensor Middleware and Application in Internet of Things (IoT). International Distributed Sensor Networks [Online], https://doi.org/10.1155/2016/2965438

[24] N. Park, J. Kwak, S. Kim, D. Won & H. Kim. (2006). WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment. *Advanced Web and Network Technologies, and Applications, LNCS,* 741-748.

[25] N. Park & N. Kang. (2015). Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle. *Sensors, 16(1),* 1-16.

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

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

[28] J. Kim & N. Park. (2019). Lightweight knowledge-based authentication model for intelligent closed circuit television in mobile personal computing. *Personal and Ubiquitous Computing,* 1-9.

[29] N. Park, Y. Sung, Y. Jeong, S. B. Shin & C. Kim. (2018). The Analysis of the Appropriateness of Information Education Curriculum Standard Model for Elementary School in Korea. *International Conference on Computer and Information Science, 791,* 1-15.

[30] W. H. Lee, J. Y. Hahm, H. M. Jung & K. M. Jeong. (2019). Traffic Data Generation Technique for Improving Network Attack Detection Using Deep Learning. *Journal of the Korea Convergence Society, 10(11),* 1-7.

[31] N. Park. (2017). The Development of Financial Engineering Expert STEAM Program based on Creative Mechanical Engineering Design. *Information, 20(2B),* 1147-1154.

[32] J. M. Lim. (2019). The Effect of Digital Signage Content Appeal Type and Interactivity on Attitude and Memory. *Journal of Digital Convergence, 17(11),* 21-27.

[33] P. S. Jeong & Y. H. Cho. (2019). Smart Factory Safety Management System using Bluetooth. *Journal of the Korea Convergence Society, 10(11),* 47-53.

[34] D. Y. Lee, D. H. Kim, S. J. Jo & H. S. Kang. (2019). Research on Development and Operation of Flipped Learning Based Learner-Centered Science Gifted Education Program. *Journal of Digital Convergence, 17(11),* 81-89.

[35] B. Jung. (2019). Performance Evaluation of Caching in PON-based 5G Fronthaul. *Journal of Convergence for Information Technology, 10(1),* 22-27.

[36] M. S. Kim. (2019). The Effects of Personality Traits and Social Support on Teacher's Efficacy of Early Childhood Teachers. *Journal of Convergence for Information Technology, 10(1),* 169-177.

김 희 경(HeeKyung Kim) [학생회원]

· 1990년 2월 : 제주대학교 과학교육학과 (이학사)
· 1992년 4월 ~ 현재 : 제주특별자치도 교육청 근무
· 2018년 3월 ~ 현재 : 제주대학교 대학원 융합정보보안학협동과정 석사과정
· 관심분야 : 블록체인, 인공지능, 빅데이터, SW교육 등
· E-Mail : baulyna@korea.kr

박 남 제(Namje Park) [정회원]

· 2008년 2월 : 성균관대학교 컴퓨터공학과(공학박사)
· 2003년 4월 ~ 2008년 12월 : 한국전자통신연구원(ETRI) 정보보호연구단 선임연구원
· 2009년 1월 : University of California at LA(UCLA) Post-Doc.
· 2010년 1월 : Arizona State University (ASU) Research Scientist
· 2010년 9월 ~ 현재 : 제주대학교 교육대학 초등컴퓨터교육전공 교수, 대학원 융합정보보안협동과정 학과장, 사이버보안인재교육원장, 창의교육거점센터장
· 관심분야 : 정보교육, STEAM, 정보보호, 암호이론 등
· E-Mail : namjepark@jejunu.ac.kr