KIPS Trans. Softw. and Data Eng.
Vol.9, No.11 pp.351~356
ISSN: 2287-5905 (Print), ISSN: 2734-0503 (Online)

https://doi.org/10.3745/KTSDE.2020.9.11.351

Blockchain-Based Access Control Audit System for Next Generation Learning Management

Ji Young Chun† · Geontae Noh††

ABSTRACT

With the spread of COVID-19 infections, the need for next-generation learning management system for undact education is rapidly increasing, and the Ministry of Education is planning future education through the establishment of fourth-generation NEIS. If the fourth-generation NEIS System is well utilized, there are advantages such as providing personalized education services and activating the use of educational data, but a solution to the illegal access problem in an access control environment where strict authorization is difficult due to various user rights. In this paper, we propose a blockchain-based access control audit system for next-generation learning management. Sensitive personal information is encrypted and stored using the proposed system, and when the auditor performs an audit later, a secret key for decryption is issued to ensure auditing. In addition, in order to prevent modification and deletion of stored log information, log information was stored in the blockchain to ensure stability. In this paper, a hierarchical ID-based encryption and a private blockchain are used so that higher-level institutions such as the Ministry of Education can hierarchically manage the access rights of each institution.

Keywords : Next Generation Learning Management System, Blockchain, Access Control, Audit System

차세대학습관리를 위한 블록체인 기반의 접근제어 감사시스템

천 지 영† · 노 건 태††

요 약

COVID-19 감염증의 확산으로 언택트 교육을 위한 차세대학습관리시스템의 필요성이 빠르게 증가하고 있으며, 교육부는 4세대 나이스 구축을 통해 미래 교육을 계획하고 있다. 4세대 나이스 시스템이 잘 활용되었을 경우, 맞춤형 교육 서비스 제공, 교육데이터 이용 활성화 등의 장점이 존재하나, 사용자의 권한이 다양하여 엄격한 권한부여가 힘든 접근제어 환경에서 불법적인 접근 문제를 해결할 수 있는 방안이 필요하다. 본 논문에서 우리는 차세대학습관리를 위한 블록체인 기반의 접근제어 감사시스템을 제안한다. 제안하는 시스템을 통해 민감한 개인정보는 암호화하여 저장하고, 추후 감사자가 감사를 수행할 때 복호화에 필요한 비밀키를 발급함으로써 원활한 감사가 이루어지도록 한다. 또한, 저장된 로그 정보의 위·변조 및 삭제 등을 방지하기 위해 로그 정보를 블록체인에 저장하여 안정성을 확보하였다. 이를 위해 계층적 ID 기반 암호와 프라이빗 블록체인을 사용하여 교육부와 같은 상위 기관에서 각 기관의 접근권한을 총괄적으로 관리할 수 있도록 구성한다.

키워드 : 차세대학습관리시스템, 블록체인, 접근제어, 감사시스템

1. 서 론

4차 산업혁명 시대의 기술인 클라우드, 인공지능, 빅데이터, 블록체인 등을 교육에 적용하려는 움직임이 최근 COVID-19 감염증의 확산으로 인해 더욱 가속화되고 있다. COVID-19 감염증의 유행으로 인해 2020년 1학기에 초중고 및 대학교의 개학이 불가능해지자 우리나라에서는 최초로 온라인 개학을 실시하였다. 학생들은 EBS 온라인 클래스나 구글 클래스룸, 화상회의 등을 통하여 온라인 수업을 실시하고 있고, 대부분의 수업이 온라인으로 진행되면서 과제, 시험, 평가와 같은 많은 부분들이 온라인으로 이루어지고 있다. 따라서 이러한 시대적 흐름에 맞춰 언택트(Untact) 교육을 위한 차세대 학습관리시스템의 필요성이 대두되고 있다.

교육부에서도 4차 산업혁명 시기에 선제적 대응을 준비하기 위해 교육행정 서비스 고도화를 도모하고 있으며, 이에 대한 일환으로 2,000억 원이 넘는 대형 사업인 4세대 나이스(NEIS, National Education Information System) 구축을 통해 미래 교육을 계획 중에 있다[1]. 교육정보시스템인 나이스는 성적처리, 출결 등 교육행정 및 교무업무를 전자적으로 연계 처리하기 위하여 교육부 및 시·도 교육청에서 설치하여 운영 중인 시스템이다[2]. 교육부에서는 나이스와 이원화된 '학교수업지원플랫폼'을 구축하여 학교수업지원플랫폼의 과정중심평가 결과를 나이스와 연계하여 학교생활기록에 활용할 예정이다[1].

이러한 시스템이 잘 활용되었을 경우 맞춤형 교육 서비스 제공, 교육데이터 이용 활성화 등의 장점이 있으나, 안전한 교육정보 체계의 구축 또한 요구된다. 지난 2018년 대비 2019년에는 교육기관시스템 사용자의 패스워드를 알아내려는 무작위 대입 공격(Brute Force Attack)이 23% 증가하였고, 프로그램 취약점을 악용한 공격 시도가 전체 중 54%로

† 정 회 원 : 이화여자대학교 컴퓨터공학전공 특임교수
†† 비 회 원 : 서울사이버대학교 빅데이터·정보보호학과 조교수
Manuscript Received : October 14, 2020
Accepted : October 28, 2020
* Corresponding Author : Geontae Noh(gnoh@iscu.ac.kr)

매우 높았다[1]. 따라서 교육기관의 정보보호에 대한 지속적인 강화 노력이 요구된다.

차세대학습관리시스템에서는 학생들에 대한 모든 온라인 활동 및 성적정보 등이 기록될 것이기 때문에 기존의 시스템보다는 강화된 보안이 필요하다. 나이스의 경우 자유학기제 및 고교학점제 등이 시행되면서 많은 외부 강사들도 시스템을 이용하게 되고, 학생, 학부모, 교사들 또한 학습관리시스템 이용 빈도가 늘어날 것이기 때문에 학생들의 개인정보에 대한 불법 조회, 수정, 유출 등을 차단하기 위한 방법이 요구된다[3]. 따라서 시스템 접근 관리를 위한 접근제어 기법이 필요하며, 각각의 사용자가 자신의 권한에 맞는 접근을 할 수 있는 적절한 권한의 부여가 필요하다.

하지만 학습관리시스템과 같이 사용자의 권한이 다양한 환경에서는 엄밀한 접근제어가 쉽지 않다. 학교의 경우를 예로 들면, 한 학생의 생활기록부에 접근할 수 있는 교사는 담임 선생님, 각 과목 선생님들, 동아리 및 방과 후 교사 등 여러 사람이 있을 것이고, 이 교사들 또한 여러 반을 가르치거나 여러 학년을 가르치는 등 간단한 권한부여로 해결하기 어려운 구조로 되어있다. 따라서 실제로 학교 일선에서는 과다한 권한이 부여되는 경우가 많다. 일례로 권한이 없는 학부모 교사가 자식의 생활기록부를 조작한 사건이 실제로 발생한 바 있다[4].

따라서 차세대학습관리시스템과 같이 엄격한 권한부여가 힘든 접근제어 환경에서 불법적인 접근 문제를 해결할 수 있는 방안이 필요하다. 이를 위한 방안으로 시스템의 로그 정보를 활용할 수 있는데, 저장된 로그 정보를 사후 감사에 이용할 수 있어 사건 발생 후 적발이 가능하게 된다. 이는 불법적인 행위가 발생하였을 때 적시에 발견하기는 어렵지만 사건 후 사후 적발이 가능하고, 이를 시스템 사용자가 누구나 인지하고 있다면 불법적인 접근에 대한 시도가 이루어지지 않을 것이다.

본 논문에서는 차세대학습관리를 위한 블록체인(Blockchain) 기반의 접근제어 감사시스템을 제안한다. 제안하는 시스템에서는 불법적인 접근에 대한 사후 적발을 위해 로그 정보를 활용하고, 이러한 로그 정보 또한 불법적으로 변조되어서는 안되므로 로그 정보를 블록체인에 올려 무결성을 보장할 수 있는 시스템을 제안한다. 학습관리시스템에서 저장되는 로그 정보에는 민감하거나 과도한 개인정보가 저장될 가능성이 있다. 예를 들어, 선생님이 학생에 대한 성적을 기록하거나 특이 사항을 기록하는 경우, 이러한 정보가 로그에 남게 된다면 개인에 대한 프라이버시 침해를 야기할 수 있다. 따라서 제안하는 시스템에서는 민감한 개인정보를 암호화한 후 저장하고, 추후 감사자가 감사를 수행할 때 복호화에 필요한 비밀키를 발급함으로써 원활한 감사가 이루어질 수 있다. 또한, 암호화에 사용하는 암호 기법으로는 계층적 ID 기반 암호(Hierarchical ID-based Encryption)를 사용하여 교육부와 같은 상위 기관에서 각 기관의 접근권한을 총괄적으로 관리하는 정보관리책임자에게 비밀키를 발급하고, 각 기관의 정보관리책임자가 정보 관리자(감사자)에게 하위 비밀키를 발급할 수 있도록 계층적인 비밀키 발급 구조를 구성함으로써 효율적인 감사가 이루어질 수 있도록 하였다.

아래의 1.1절에서는 본 논문을 이해하기 위한 배경 지식으로 개인정보보호법과 개인정보의 안전성 확보조치 기준 중 본 논문과 관련된 주요 내용을 정리한다. 이후 2장에서는 본 논문에서 우리가 제안한 시스템을 설계하는데 있어 가장 중요한 개념들인 블록체인과 계층적 ID 기반 암호에 대해 설명하고, 본 연구와 가장 관련성이 높은 연구와 비교 분석한다. 3장에서는 본 논문의 목적과 필요성으로부터 시작하여 차세대학습관리를 위한 블록체인 기반의 접근제어 감사시스템을 설계하고 분석한다. 마지막 4장에서 본 논문의 결론을 맺는다.

1.1 개인정보보호법과 개인정보의 안전성 확보조치 기준

개인정보보호법 제23조(민감정보의 처리 제한), 제24조(고유식별정보의 처리 제한), 제29조(안전조치의무), 동법 시행령 제21조(고유식별정보의 안전성 확보 조치), 제30조(개인정보의 안전성 확보 조치)에 따라 개인정보의 안전성 확보조치 기준이 법적 근거를 기반으로 마련되었다. 이에 따라 개인정보처리자 및 개인정보처리자로부터 개인정보를 제공받거나 처리를 위탁받은 자는 개인정보를 안전하게 처리할 법적 의무가 발생하며, 이는 반드시 준수해야 하는 최소한의 기준이 된다. 즉, 개인정보 처리자는 개인정보를 처리하는 경우, 해당 기준을 반드시 준수해야 한다.

본 논문에서 우리는 2019년 6월, 행정안전부와 한국인터넷진흥원(KISA)이 공동 발간한 '개인정보의 안전성 확보조치 기준 해설서'의 해석을 기반으로 시스템을 설계하고자 하며[5], 특히 제8조(접속기록의 보관 및 점검)를 만족하는 시스템을 설계하고자 한다. 제8조(접속기록의 보관 및 점검) 내용은 아래와 같다.

① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다. 다만, 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다.

② 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히 개인정보를 다운로드한 것이 발견되었을 경우에는 내부 관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다.

③ 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

'개인정보의 안전성 확보조치 기준 해설서'에 따르면, 기록하는 정보주체 정보의 경우 민감하거나 과도한 개인정보가 저장되지 않도록 하여야 한다. 또한, 개인정보를 검색하는 경우 검색조건문만을 기록한다면 DB테이블 변경 등으로 책임추적성 확보가 어려울 수 있기 때문에 책임추적성 확보를 위한 필요한 조치를 취해야 하며, 이는 책임추적성을 확보하기에 충분한 기간 동안 보관 및 관리할 수 있도록 처리해야 한다. 개인정보처리자는 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검해야 하며, 개인정보를 다운로드한 것이 발견된 경우 그 사유를 반드시 확인하게 되어 있다.

2. 관련 연구

우리는 본 장에서 우리가 제안할 시스템을 설계하는데 있어 가장 중요한 개념들인 블록체인과 계층적 ID 기반 암호에 대해 설명한다. 이후 본 논문에서 제안할 시스템과 가장 관련성이 높은 연구와 비교 분석한다.

2.1 블록체인

데이터의 무결성을 보장하기 위한 암호학적인 도구로 해시 함수(Hash Function)가 가장 널리 사용되고 있으며, 해시 함수의 특성을 기반으로 한 블록체인이 최근 10여 년간 각광을 받고 있다. 블록체인은 2008년, Satoshi Nakamoto에 의해 제안된 전자 화폐 시스템인 비트코인(Bitcoin)의 등장 이후로 최근 급격히 발전하고 있으며[6], 무결성을 보장하는 구조를 설계하기 위해 블록 사이에 해시 함수를 체인 형태로 엮은 구조적 특성을 가지고 있다.

블록체인에 업로드된 자료는 투명성을 제공하기 때문에 누구나 볼 수 있고, 누구나 검증 가능하다. 블록끼리 연결된 자료의 무결성 훼손을 방지하기 위해 해시 함수의 안전성에 기반을 두고 있다. 블록체인은 거래(Transaction)들의 집합으로 구성된 블록을 기반으로, 전자 화폐에 사용되기 위한 목적으로부터 시작하였으나, 최근에는 금융뿐만 아니라 다양한 환경에 접목하기 위한 시도들이 지속적으로 진행되고 있다.

블록체인은 모두가 참여자가 될 수 있고, 모두가 감시자가 될 수 있는 공개적 특성을 기본으로 하며, 이를 특별히 퍼블릭 블록체인(Public Blockchain)이라고 한다. 이와는 달리, 중앙 관리자가 존재하여 폐쇄적으로 운영되는 블록체인을 프라이빗 블록체인(Private Blockchain)이라고 하고, 퍼블릭 블록체인과 프라이빗 블록체인의 특성을 결합한 컨소시엄 블록체인(Consortium Blockchain)이라고 한다. 본 논문에서는 강력한 중앙 관리자가 존재하고, 데이터의 무결성 보장에 초점을 둔 프라이빗 블록체인에 초점을 두기로 한다.

2.2 계층적 ID 기반 암호

계층적 ID 기반 암호는 공개키 암호(Public Key Encryption)의 한 종류이다. 공개키 암호는 1970년대에 처음으로 등장한 개념으로, 그 이전에는 대칭키 암호만이 존재하였으나, 공개키 암호에서는 복호화할 능력이 있는 사용자가 자신의 비밀키와 공개키를 소지하고 있으며, 자신의 공개키는 누구나 볼 수 있도록 공개하고, 자신의 비밀키는 자신만이 알 수 있도록 안전하게 관리한다. 암호화하고자 하는 사용자는 복호화할 능력이 있는 사용자의 공개키를 사용하여 메시지를 암호화하며, 복호화할 능력이 있는 사용자는 자신의 비밀키를 사용하여 암호문을 복호화한다.

공개키 암호에서 사용되는 공개키와 비밀키는 일반적으로 난수적 특성을 가지며, 따라서 특정 공개키가 어느 사용자의 것인지를 알기 위해서는 PKI(Publikc Key Infrastructure)와 같은 신뢰기관이 존재해야 한다. 이러한 특성을 해소하기 위해 ID 기반의 암호(ID-based Encryption)가 등장하였으며, ID 기반의 암호는 사용자의 공개키가 사용자의 이메일과 같이 식별이 수월한 형태를 가진다는 특징이 있다[7, 8]. ID 기반의 암호는 공개키 암호에서와는 달리 PKI가 존재할 필요가 없으나, 비밀키를 생성하기 위한 KGC(Key Generation Center)가 필요하다는 특성이 있다. 즉, 형태와 역할은 다르지만 여전히 신뢰기관은 필요하다.

계층적 ID 기반 암호는 ID 기반 암호의 확장된 형태로, 특정 사용자가 구조적으로 자신의 하위 계층에 존재하는 사용자들에게 비밀키를 발급해줄 수 있는 트리 구조를 가진다[9, 10]. 즉, 최상위 계층의 사용자는 여전히 KGC를 통해 비밀키를 생성해야 하지만, i+1 계층의 사용자는 i 계층에 있는 자신의 부모 노드 사용자로부터 비밀키를 발급받을 수 있다.

계층적 ID 기반 암호는 트리 구조에서 자신의 자손 노드 사용자들의 비밀키를 만드는 것이 가능하기 때문에 계층적 관리가 필요한 경우 유용하게 사용될 수 있으며, 트리 구조에서 자신의 자손 노드 사용자가 아닌 경우, 비밀키와 관련된 정보를 얻을 수 없다. 따라서 계층적 트리 형태로 구성된 구조에 사용하기에 매우 적합하다.

본 논문에서 사용할 계층적 ID 기반 암호는 아래와 같이 4가지 알고리즘으로 구성되어 있다.

- $HIBE.Set(1^n, 1^d)$: 시큐리티 파라미터 n과 계층의 깊이 d를 입력으로 받아 공개 파라미터 PP와 마스터키 mk를 생성한다.
- $HIBE.Ext(PP, sk_{id_P}, id_C)$: 퍼블릭 파라미터 PP와 부모 노드 사용자의 비밀키 sk_{id_P}, 자식 노드 사용자의 ID id_C를 입력으로 받아 자식 노드 사용자의 비밀키 sk_{id_C}를 발급한다. 만약 부모 노드가 없는 경우, sk_{id_P} 대신 마스터키 mk를 사용한다.
- $HIBE.Enc(PP, id, m)$: 퍼플릭 파라미터 PP와 복호화할 사용자의 ID id, 메시지 m을 입력으로 받아 암호문 ct를 생성한다.
- $HIBE.Dec(PP, sk_{id}, ct)$: 퍼플릭 파라미터 PP와 복호화할 사용자의 비밀키 sk_{id}, 암호문 ct를 입력으로 받아 메시지 m을 복호화한다.

2.3 관련 연구

2020년, Guangsheng Yu 등은 블록체인에서 접근제어가 가능한 시스템을 설계하였다[11]. 해당 논문에서는 접근 권한이 있는 사용자들만 블록체인에 업로드된 자료를 볼 수 있고, 그렇지 않은 사용자들은 블록체인에 업로드된 자료를 볼 수 없도록 구성하였으며, 이에 따라 데이터 체인(Data Chain)을 구성하여 자료를 업로드할 때 암호화하도록 하였다. 해당 논문의 암호화는 속성 기반 암호(Attribute-based Encryption)를 사용하여 진행하였으며, 속성 기반 암호를 통해 속성 권한이 허용되는 사용자만이 복호화 권한을 가지도록 하였다. 복호화 권한이 있는 사용자가 자신의 권한을 이용하여 비밀키를 가져오기 위해서 키 체인(Key Chain)을 구성하여 접근 권한이 있는 경우에 한해 비밀키를 검색해갈 수 있도록 구성하였다.

추가로, [11] 논문에서는 수정 가능한 블록체인(Redactable Blockchain)을 구성하기 위해 블록을 연결하는 해시 함수를 카멜레온 해시 함수(Chameleon Hash Function)를 사용하였다. 수정 가능한 블록체인은 2017년, Giuseppe Ateniese 등의 연구로부터 시작되었으며[12], 잊힐 권리(The Right to

be Forgotten)와 맞물려 최근 조금씩 논의가 진행되기 시작하였으나, 본 논문에서 제안하는 감사시스템에서는 수정 가능한 블록체인 구조가 바람직하지 않다.

본 논문에서 우리는 블록체인을 사용하여 계층적 권한 구조를 가진 형태에서 사용 가능한 감사시스템을 구성한다. 기존의 논문 [11]과 비교하여 본 논문은 감사시스템의 목적을 달성하기 위하여 속성 기반의 접근 구조가 아니라 계층적 구조를 고려하여 설계하였으며, 이에 따라 상급 기관이 하급 기관의 감사 기록을 확인하는 것이 구조적으로 가능하다. 또한, 수정 가능한 블록체인은 감사시스템에서 만큼은 결코 제공되어서는 안 되는 기능으로, 블록체인의 가장 주된 목적인 무결성을 감사시스템에서도 만족할 수 있도록 설계하였다. 그리고 기존의 논문 [11]에서는 데이터를 저장하는 체인과는 별도로, 접근 권한 관리를 위해 키를 저장하는 체인을 추가로 구성하였는데, 본 논문에서 우리는 단일 체인만으로도 원하는 목적을 달성할 수 있도록 감사시스템을 구성하였다(Table 1. 참고).

2020년, 김희경과 박남제는 교육행정정보시스템 학교생활기록부 데이터의 안정성을 확보하기 위해 블록체인 기반의 안전한 생활기록부 데이터 보호 방안을 제시하였다[13]. 해당 논문에서는 생활기록부의 기록을 블록체인에 암호화하여 기록하는 방안을 제안하였으나, 해당 논문에서 제시한 방안에는 암호학적인 구체적 설계가 이루어지지 않았고, 감사시스템을 설계하는 본 논문의 목적과는 다소 차이가 존재한다.

Table 1. Comparison of [11] and Ours

	[11]	Ours
Access Structure	Attribute	Hierarchical
Redactable	O	X
# of Chains	2 (Data Chain, Key Chain)	1

3. 제안하는 시스템

우리는 본 장에서 기존 학습관리시스템의 문제점을 먼저 살펴본 뒤, 제안하는 시스템을 구성하고 분석한다.

3.1 기존 학습관리시스템의 문제점

경상북도교육청정보센터에서는 2020년 4월, 교육정보시스템 권한부여 핸드북(나이스, K-에듀파인)을 발간하였다[14]. 해당 핸드북은 일선 학교 선생님들이 교육정보시스템의 권한부여 작업과 방법들을 설명하기 위해 제작되었으며, 나이스와 K-에듀파인에서 권한 관리를 이해하고, 권한부여에 관한 내용들이 기술되어 있다. 본 핸드북에 따르면, 메뉴 및 자료 권한은 사용자그룹이나 서브시스템별·단위업무별로 부여 가능하다. 교무업무 권한 관리의 경우, 학년 시작 전 기관 마스터 ID를 가진 권한 담당자가 각 업무 담당자에게 권한을 부여하고, 업무 담당자가 역할을 편성하는 형태로 구성된다. 일련의 다양한 권한 처리 과정에서 권한이 과다 부여될 수 있으므로 주의하도록 기술되어 있다.

2018년에는 교육부와 한국교육학술정보원(KERIS)에서 공동으로 2018년 나이스 학교관리자 연수 교재를 발간하였다[2]. 해당 교재에 따르면, 기관장(학교장)이 기관정보관리책임자로 자동 지정되며, 기관정보관리책임자는 기관정보관리자를 지정하여 기관마스터 및 권한 관리 업무를 위임할 수 있도록 하고 있으며, 업무의 편의나 관행을 이유로 담당이 아닌 교사에게 입력 및 정정 권한을 부여하지 않도록 주의하고 있다. 실제로 해당 교재에서는 실제 학교에서 전체 사용자그룹에 대해 담임 권한을 포함한 모든 권한을 부여한 과다 부여 사례를 소개하고 있으며, 이를 방지하기 위해 적정 권한을 설정하는 예시를 안내하고 있다.

실제로 현재 나이스를 통해 권한이 없는 사용자가 접속하거나 내용을 수정하는 등의 악의적인 행동을 취하는 것은 불가능하다. 다만, 나이스 접속 권한을 부여하는 기관정보관리책임자 또는 기관정보관리자가 악의적으로 권한이 없는 교사에게 임의로 권한을 주는 경우에는 막을 수 없다.

3.2 제안하는 시스템

본 논문에서는 차세대학습관리를 위한 블록체인 기반의 접근제어 감사시스템을 제안한다. 제안하는 시스템은 학생들에 대한 모든 기록이 집중되는 언택트 교육을 위한 차세대학습관리시스템에서 학생의 개인정보에 대한 안전한 접근제어가 이루어질 수 있도록 접속정보를 감사하는 시스템이다. 이러한 감사시스템의 정보를 활용하여 불법적인 접근에 대한 능동적인 대처가 가능하다. 또한, 기존의 학습관리시스템에서 발생했던 문제점들을 해결하고, 불법적인 로그 정보 수정에 대해 무결성을 보장할 수 있는 방안으로 블록체인을 활용한다.

1) 시스템 구성요소

제안하는 시스템에서 구성요소는 다음과 같다.

- 차세대학습관리시스템 관리자(TA; Trusted Authority): 전체 시스템을 관리하는 관리자로, 각 기관의 접근권한을 총괄적으로 관리한다. 나이스 시스템의 경우 나이스 시스템의 접근권한을 총괄적으로 관리하는 사람을 의미한다.
- 개인정보관리책임자(CPO; Chief Privacy Officer): 각 기관에서 사용자의 개인정보를 보호·관리하는 최고 책임자로 각 기관의 학습관리시스템의 접근권한을 관리한다. 따라서 자신이 관리하는 학습관리시스템의 감사를 위해 지정한 감사자에게 감사 권한을 부여한다. 나이스 시스템의 경우 사용자의 업무분장에 따라 소속 기관의 나이스 접근권한을 부여・회수하는 기관권한관리자(기관정보관리책임자 또는 기관정보관리자)가 이에 해당한다.
- 감사자(Auditor): 각 기관의 학습관리시스템에 대한 접근기록을 감사하는 역할을 담당한다. 개인정보보호법에 따라 시스템에 대한 접속기록을 월 1회 이상 점검할 의무를 가진다. 나이스 시스템의 경우 개인정보처리자가 이에 해당한다.
- 사용자(User): 차세대학습관리시스템을 이용하는 사람들을 총칭하며, 나이스 시스템의 경우 학생, 학부모, 교사 등이 이에 해당한다.

2) 로그 정보 생성

개인정보의 안전성 확보조치 기준 제8조(접속기록의 보관

및 점검)에 부합하는 접속기록을 저장한다. 기록하는 정보의 예시는 다음과 같다.

- 계정: A0001
- 접속일시: 2019-02-25, 17:00:00
- 접속지 정보: 192.168.100.1
- 처리한 정보주체 정보: CLI060719
- 수행업무: 회원목록 조회, 수정, 삭제, 다운로드 등

위의 정보는 반드시 기록하여야 하는 정보이며, CPO는 업무환경에 따라 책임추적성 확보에 필요한 항목을 추가로 기록해야 한다. 또한, 검색조건문(데이터베이스 쿼리)를 통하여 대량의 개인정보를 처리했을 경우 해당 검색조건문을 정보주체 정보로 기록할 수 있다. 하지만 이런 경우 추후 데이터베이스 테이블이 변경되었을 때 책임추적성의 확보가 어려우므로 해당 시점의 데이터베이스 백업이 필요하다.

데이터베이스 백업의 경우 데이터베이스 보관에 대한 규정이 명확히 존재하지 않으므로 본 논문에서는 로그 정보에 필요한 데이터베이스 정보를 저장하는 것을 제안한다. 따라서 위의 필수 정보에 추가적으로 다음과 같은 정보를 저장한다.

- 책임추적성 확보를 위한 추가 정보: 개인정보의 처리에 대한 정당한 사유가 될 수 있는 해당 시점의 데이터베이스 정보

위의 추가 정보의 경우 개인정보를 포함하고 있으므로 기타 다른 로그 정보들과 함께 로그에 원문 그대로 기록하는 것은 정보주체의 프라이버시 침해 위험이 있다. 따라서 본 책임추적성 확보를 위한 추가 정보의 경우에는 계층적 ID 기반 암호를 사용하여 암호화한 후 로그에 저장하여 권한이 있는 관리자만이 필요시 추가 로그 정보를 복호화하여 볼 수 있도록 한다. 추가 로그 정보를 암·복호화하기 위한 절차는 다음과 같다.

① TA는 $HIBE.Set(1^n, 1^d)$을 실행하여 공개 파라미터 PP와 마스터키 mk를 생성한다.

② TA는 CPO의 비밀키를 생성하기 위해 공개 파라미터 PP, 자신의 마스터키 mk와 CPO의 아이디 id_{CPO}를 입력으로 $HIBE.Ext(PP, mk, id_{CPO})$를 실행하여 CPO의 비밀키 $sk_{id_{CPO}}$를 얻는다.

③ TA는 CPO에게 비밀키 $sk_{id_{CPO}}$를 부여함으로써 학습관리시스템에 대한 접근권한을 위임한다.

④ TA에게 비밀키를 부여받은 CPO는 감사자의 비밀키 생성을 위해 공개 파라미터 PP, 자신의 비밀키 $sk_{id_{CPO}}$와 감사자의 아이디 id_A를 입력으로 $HIBE.Ext(PP, sk_{id_{CPO}}, id_A)$를 실행하여 감사자의 비밀키$sk_{id_A}$를 얻는다.

⑤ CPO는 감사자에게 비밀키 sk_{id_A}를 부여함으로써 학습관리시스템에 대한 감사권한을 위임한다.

⑥ 학습관리시스템에서 로그를 자동 생성하는 프로그램은 책임추적성 확보를 위한 추가 정보인 m을 암호화하기 위해 공개 파라미터 PP, 감사자의 아이디 id_A와 추가 정보 m을 입력으로 $HIBE.Enc(PP, id_A, m)$를 실행하여 암호문 ct를 생성한다. 이와 같이 생성된 암호문 ct를 해당 접속에 대한 필수 로그 정보들과 함께 로그에 저장한다.

⑦ 추후 정기적인 감사를 위해 로그 정보에 대한 분석이 필요하면 감사자는 자신의 비밀키 sk_{id_A}로 암호문 ct를 복호화하여 접속이 타당한지 확인한다.

⑧ 개인정보의 안전성 확보조치 기준 제8조(접속기록의 보관 및 점검)에 따라 TA가 여러 개의 학습관리시스템을 통합하여 점검할 수 있어야 하기 때문에 TA는 자신의 마스터키 mk를 이용하여 여러 개의 학습관리시스템의 로그를 복호화할 수 있어야 한다. 제안하는 기법에서는 계층적 ID 기반 암호를 사용하였기 때문에 감사자의 비밀키를 발급한 상위 기관인 TA가 감사자의 아이디를 사용하여 암호화된 암호문을 복호화할 수 있다.

3) 블록체인에 등록

개인정보의 안전성 확보조치 기준 제8조(접속기록의 보관 및 점검)에 따라 개인정보에 대한 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다. 따라서 제안하는 기법에서는 생성된 로그 정보를 프라이빗 블록체인에 기록한다. 제안하는 시스템에서는 TA라는 중앙 관리자가 존재하기 때문에 여러 가지 블록체인 형태 중 프라이빗 블록체인의 사용이 가장 적합하다.

블록체인에 올린 데이터는 무결성을 보장받기 때문에 접속기록이 위·변조로부터 안전하다. 또한, 블록체인 데이터는 P2P(Peer-to-Peer) 네트워크를 통해 분산 저장되기 때문에 도난 및 분실로부터 안전하다.

4. 분 석

제안하는 시스템은 접근권한의 부여가 너무 복잡하여 엄밀한 접근제어를 할 수 없는 상황에서 접근권한의 오·남용을 사후 감사할 수 있다. 개인정보 접근에 대한 책임추적성 확보를 위해 필요한 추가적인 정보를 암호화하여 남김으로써 사후 불법적인 접근에 대한 적발이 가능하도록 조치함으로써 사용자 스스로 불법적인 접근을 할 수 없도록 하는 효과를 가진다. 또한, 실시간으로 로그 정보를 분석한다면 불법적인 접근에 대해 실시간 파악이 가능하고 이에 대한 적절한 대응이 가능하게 된다.

추가적으로 저장하는 접속정보에는 민감하거나 과다한 개인정보가 저장될 수 있기 때문에 이러한 정보를 암호화한 뒤 저장하여 권한이 있는 관리자만 암호문을 복호화할 수 있게 된다. 또한, 기관의 감사자나 관리자뿐만 아니라 권한을 위임한 상위 기관에서도 감사가 가능하도록 계층적 ID 기반 암호를 사용하여 계층적인 관리가 가능하다. 계층적 ID 기반 암호의 안전성에 따라 하위 기관에서는 권한을 부여한 상위 기관의 비밀 정보를 볼 수 없다.

저장되는 로그 정보는 위·변조 및 도난, 분실되어서는 안된다. 만약 이와 같은 일이 발생한다면, 악의적인 사용자가 불법적인 접속을 한 후 자신의 접속 기록을 지워 감사가 사후 적발이 불가능하도록 할 수 있기 때문이다. 하지만 제안하는 시스템에서는 로그 정보를 프라이빗 블록체인에 저장하여 로그 정보에 대한 무결성을 확보하였으며, 블록체인 환경에서는 로그 정보가 분산되어 저장되기 때문에 도난 및 분실이 불가능하다.

5. 결 론

본 논문에서 우리는 차세대학습관리를 위한 블록체인 기반의 접근제어 감사시스템을 제안하였다. 학습관리시스템과 같이 사용자의 권한이 다양한 환경에서는 엄밀한 접근제어가 쉽지 않으며, 학교의 경우에도 간단한 권한부여로 해결하기 어려운 구조로 되어있어서 실제로 일선에서 과다한 권한이 부여되는 경우가 많다.

우리가 제안한 시스템을 통해 민감한 개인정보는 계층적 ID 기반 암호를 사용하여 암호화 후 저장하고, 추후 감사자가 감사를 수행할 때 복호화에 필요한 비밀키를 상위 계층에서 발급함으로써 원활한 감사가 이루어지도록 한다. 또한, 저장된 로그 정보의 위·변조 및 삭제 등을 방지하기 위해 로그 정보를 블록체인에 저장하여 안정성을 확보하였다.

본 논문에서 제안하는 시스템을 활용하면 교육부와 같은 상위 기관에서 각 기관의 접근권한을 총괄적으로 관리할 수 있으며, 이를 통해 보다 투명한 차세대학습관리가 가능해질 것으로 기대한다.

References

[1] “2020 Education Information Service Implementation Plan,” Ministry of Education, Education Safety Information Office, 2020.

[2] “2018 NEIS School Manager Training Textbook,” Ministry of Education, KERIS(Korea Education & Research Information Service), 2018.

[3] M. H. Yu, “Ministry of Education Strengthens Security System for Fourth Generation ‘NEIS System’ of Education Administration Information System,” 2019.

[4] “Leaked Test Papers, Manipulated Life Records... "How do you Believe in High School?,” The Korea Economic Daily, 2018.

[5] “Personal Information Specification for Security Assurance Measures,” Ministry of the Interior and Safety, KISA(Korea Information Security Agency), 2009.

[6] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[7] A. Shamir, “Identity-based Cryptosystems and Signature Schemes,” Advances in Cryptology - CRYPTO 1984, LNCS 196, pp.47-53, 1985.

[8] D. Boneh and M. Franklin, “Identity-based Encryption from the Weil Pairing,” Advances in Cryptology - CRYPTO 2001, LNCS 2139, pp.213-229, 2001.

[9] J. Horwitz and B. Lynn, “Toward Hierarchical Identity-based Encryption,” Advances in Cryptology – EUROCRYPT 2002, LNCS 2332, pp.466-481, 2002.

[10] C. Gentry and A. Silverberg, “Hierarchical Id-based Cryptography,” Advances in Cryptology - ASIACRYPT 2002. LNCS 2501, pp.548-566, 2002.

[11] G. Yu, X. Zha, X. Wang, W. Ni, K. Yu, P. Yu, J. A. Zhang, R. P. Liu, and Y. J. Guo, “Enabling Attribute Revocation for Fine-Grained Access Control in Blockchain-IoT Systems,” *IEEE Transactions on Engineering Management*, pp.1-18, 2020.

[12] G. Ateniese, B. Magri, D. Venturi, and E. R. Andrade, “Redactable Blockchain - or - Rewriting History in Bitcoin and Friends,” in *Proceedings of 2017 IEEE European Symposium on Security and Privacy*, pp.111-126, 2017.

[13] H. Kim and N. Park, “Design and Implementation of Blockchain for Securing Data of National Education Information System School Life Records,” *Journal of the Korea Convergence Society*, Vol.11, No.3, pp.27-35, 2020.

[14] “Education Information System Authorization Handbook (NEIS, K-Edufine),” Gyeongsangbuk-do Office of Education Information Center, 2020.

천 지 영

https://orcid.org/0000-0002-5329-8918
e-mail : jychun@ewha.ac.kr
1997년 이화여자대학교 수학과(학사)
2006년 고려대학교 정보보호학과(석사)
2011년 고려대학교 정보경영공학과(박사)
2011년 ~ 2019년 고려대학교 정보보호연구원 연구교수
2020년 ~ 현 재 이화여자대학교 컴퓨터공학전공 특임교수
관심분야 : 암호 프로토콜, 빅데이터 보안, 프라이버시 향상 기술

노 건 태

https://orcid.org/0000-0003-2547-7529
e-mail : gnoh@iscu.ac.kr
2008년 고려대학교 산업시스템정보공학과 (학사)
2010년 고려대학교 정보경영공학과(석사)
2014년 고려대학교 정보보호학과(박사)
2014년 ~ 2017년 고려대학교 정보보호연구원 연구교수
2017년 ~ 현 재 서울사이버대학교 빅데이터·정보보호학과 조교수
관심분야 : 암호 이론, 데이터 보안, 프라이버시 향상 기술