Journal of Next-generation Convergence Information Services Technology Vol.10, No.1, February (2021), pp.33-43
ISSN 2384-101X(p) 2672-1163(e) *http://dx.doi.org/10.29056/jncist.2021.02.04*

DID기반 대학교 개인정보 보호의 필요성

Necessity of DID-based Personal Information Protection in Domestic University

윤원석[1], 심미나[2]*

Won-Seok Yoon[1], Mina Shim[2]*

요 약

본 논문은 국내의 여러 대학교에서의 지속적인 개인정보 유출사건이 발생됨으로 인해 해당 대학교의 이미지 실추 및 엄청난 경제적인 손실을 초래하므로 대학교의 개인정보를 보호하는 방법에 대해 조사하고 이에 대한 개인정보 보호 및 관리의 문제점을 분석해 DID(Decentralized Identifier)기반으로 국내 대학교의 개인정보를 보호해야하는 필요성을 제시하는데 목적이 있다. 이를 위해 개인정보를 유출당한 대학교들의 대표적인 최근 사례가 내부에서 일어나는 유출과 외부의 악의적인 방식을 통해서 일어나는 사례를 조사해 개인정보 유출을 통한 피해 량을 분석한다. 대학교 개인정보 유출로 인한 피해를 줄이기 위해 현재 국내의 대학교 종합정보 시스템의 구조를 분석해 대학교의 정보보안 시스템이 취약하다는 점을 밝히고 해당 취약점은 DID 기반의 탈중앙화 신원증명을 통해서 학생 및 교수의 개인정보를 학교의 중앙화된 시스템에 보호하는 것이 아니라 개인의 신원을 사용자가 직접 관리하여 인증하는 방식인 블록체인 기반의 DID의 필요성에 대해 제언한다.

핵심어 : 블록체인, 탈중앙화, 신원증명, 개인정보 보호

Abstract

Due to the continuous leakage of personal information at various universities in Korea, the image of the university is deteriorated and a huge economic loss is caused. Therefore, the purpose of this thesis is to investigate how to protect personal inforation of universities, analyze current problems of personal information protection and management, and present the need to protect personal information of domestic universities based on DID (Decentralized Identifier). have. To this end, it is revealed that the university's information security system is weak by analyzing the representative recent cases of universities that have leaked personal information from interior and the exterior. In addition, it proposes the necessity of blockchain-based DID, which is a method in which the personal information of students and professors is not protected by a centralized system, but the user's personal identity is directly managed and authenticated.

Keyword : Blockchain, Decentralization, Identification, Personal Information Protection

1 Department of Computer Engineering, Sungkyul University, Gyeonggi, Korea [Undergraduate Students]
e-mail: wonseok3629@gmail.com
2 Department of Computer Engineering, Sungkyul University, Gyeonggi, Korea [Professor]
e-mail: mnshim@sungkyul.ac.kr (Corresponding author)
* 이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2019R1F1A1060564).

Received(January 2, 2021), Review Result(1st: January 22, 2021), Accepted(February 5, 2021), Published(February 28, 2021)

1. 서론

4차 산업혁명이 다가오면서 정보화 사회에서 정보통신 매체가 기업 및 사회에 차지하는 비중이 급격하게 증가함에 따라 개인ID를 악용한 전자문서 위변조, 사기, 명의 도용 등 개인정보 유출로 인해 신체상의 피해, 재산상의 피해등 사회적 위험이 전 세계적으로 문제되고 있다. 개인정보 유출로 인한 사이버 공격의 위험은 기업뿐만 아니라 전국 대학교에서도 다양하게 문제가 되고 있다. 현재 국내 대학의 학생, 대학 교직원에 대한 막대한 양의 개인정보와 대학의 중요한 연구기록 정보들은 모두 대학교의 서버에 기록되어 보관되어지고 있다. 하지만 이러한 중요한 정보를 보유하고 있는 대학교의 전산망시스템이 사이버 위협에 항상 노출되어 매우 취약해 국내의 대학들의 개인정보들이 유출되고 있는 것이 현실이다. 해당 대학의 사이버 공격을 통해 약 3만 여명의 학생 및 교직원들의 이름, 포털 아이디, 이메일, 학과, 학번의 개인정보가 유출된 사건이 있었고, 대학의 전산망을 공격해 졸업자의 이름, 주소, 전화번호, 직장명 등의 개인정보를 유출당한 사건이 있었다. 이렇듯 국내 대학의 취약한 보안으로 인해 대학 내의 학생 및 교직원들의 중요한 개인정보가 유출될 수 있으므로, 본 논문에서는 개인에 대한 정보를 중앙 서버에 보관하는 것이 아니라 블록체인 기반의 DID(Decentralized Identity)에 보관하여 개인정보를 보호하고 인증하는 것에 대한 필요성을 제언하고자 한다.

2. 관련연구

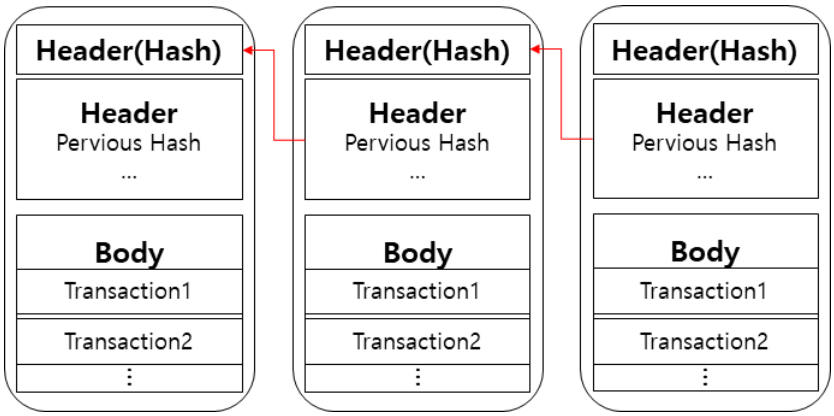
2.1 개인정보 침해 요인 분석

조직 내 내부자들의 불법 유통 증가와 다양한 공격을 통한 외부 해커의 위협이 증가하고 면서 개인의 자기정보에 대한 가치 인식이 점차 변화함에 따라 개인정보 처리에 대한 실태를 파악하고 침해요인을 분석하는 연구들이 다양하게 진행되고 있다. 4차 산업혁명이 진행되면서 AI(Artifical Intelligence), IOT(Internet Of Thing), 블록체인 등과 같은 신기술에 대한 개발과 서비스가 늘어나면서 데이터 수요의 급격한 증가 현상이 나타나고 있다. 이로 인해 개인정보에 대한 사이버 공격을 받는 피해와 분야별 서비스의 개인정보 처리의 실태를 파악하고 침해 가능한 요소들을 찾아 각 서비스별로 개인정보의 개별적인 보호조치가 필요하다는 연구가 진행되었으며 [1], 학생 및 교원들의 개인정보 관리에 대해서 분석하고 대학교의 행정의 개념과 행정 업무에 대해서 분석해 학생 및 교원들의 개인정보를 대학교에서 어떻게 수집하고 생성하며 중앙화된 대학교 시스템의 개인정보 보호의 취약점과 관리 실태를 파악해 대학교 개인정보 유출 방지를 위한 개선방안을 제언하는 연구가 진행되었다[2].

본 논문은 기존에 연구되어 왔던 중앙화된 전산망 구조 시스템의 개인정보 관리의 중요성 연구와 달리 블록체인 기술을 활용하여 탈중앙화된 개인정보 보호 및 관리 시스템을 제언하면서 DID 기반의 대학교 개인정보 보호의 필요성에 대해서 설명한다.

2.2 블록체인

블록체인은 2008년의 사토시 나카모토 저자의 논문인 탈중앙회된 개인과 개인의 전자상의 거래 연구에서 처음 실증하였고 현재의 4차 산업혁명 신기술의 핵심중 하나인 블록체인 기술까지 발전을 시킨 기반이 되었다 [3]. 블록체인은 P2P(Peer to Peer)기반으로 데이터를 공동으로 관리하는 새로운 개념의 분산거래장부로 블록체인 네트워크의 모든 사용자가 공동으로 데이터를 기록하고 보관하는 기술을 의미한다. 블록체인은 정보를 암호화시켜 전송 및 기록되고 데이터를 네트워크 내의 모든 사용자들에게 분산되어 기록되기 때문에 데이터 조작 및 오류를 방지할 수 있다.



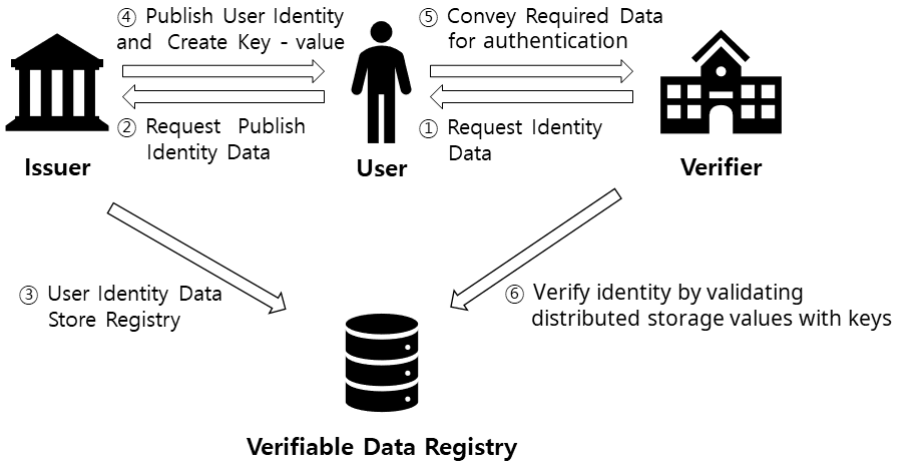
[그림 1] 블록체인 블록 구조

[Fig. 1] Block Structure of Blockchain

[그림 1]은 블록체인의 연결되어 있는 블록의 기본 구조이다. 블록은 특정 시간동안 모인 다수의 트랜잭션 집합을 바디에 넣어 해당 거래정보 넣고, 생성한 블록의 헤더에 이전의 정보를 가지고 생성되기 때문에 블록들이 서로 연결되어 추적이 가능하도록 생성하여 모든 참여자들에게 전송해 연결된 블록은 수정이 불가능하게 영구적으로 저장된다 [4]. 최근 블록체인에 관한 연구로는 블록체인 기반의 디지털화폐연구가 진행 중이고, 중앙은행의 CDBC(Central Bank Digital Currency)와 페이스북의 리브라(Libra)가 블록체인 기반의 디지털화폐 혁신의 출발점이 될 것으로 예상되고 있다 [5]. 블록체인은 디지털 화폐거래 뿐만 아니라 프라이빗 블록체인을 통해서 개인정보를 보관하는 곳에서 유출을 방지하고 보호할 수 있다 [6].

2.3 DID(Decentralized Identity)

DID는 블록체인 기술을 이용한 탈중앙화 전자신원증명 기술로 개인의 정보를 중앙집중 시스템이 아닌 개인에 의해서 관리 및 통제된다. DID를 통해서 자신이 신원 정보를 관리할 수 있고, 제출 범위와 대상을 정할 수 있는 방식이다. 블록체인을 통해서 개인정보를 분산저장하고 한쪽에서 이 개인정보를 위조하더라도 나머지 분산 저장된 개인정보와 비교를 통해서 위조여부를 확인 할 수 있다.



[그림 2] DID 기술 시스템 흐름

[Fig. 2] Decentralized Identity System Flow

[그림 2]는 W3C에서 제시하는 모델을 바탕으로 한 DID 신원 검증 구조이다 [7-9]. W3C에서는 사용자(User)들의 서명을 통해서 신원 데이터의 진위검증을 진행하고 검증의 유효성을 임의로 변경이 불가능 하다는 특징을 기반으로 한다. 사용자의 검증 가능한 정보를 제공하는 신원정보발행자(Issuer)는 사용자의 서명된 ID를 등록하고 신원을 증명하는 DIDs(Key) - DID Document(Value)값을 생성해 사용자가 서비스 제공자(Verifier)에게 인증에 필요한 부분만을 선택한 개인의 신원 정보를 전달하고, 서비스 제공자는 DIDs(Key)를 이용해서 분산 저장소(Verifiable Data Registry)에 저장된 DID Document를 검증해 신원을 확인한다. DID기반의 개인의 신원 정보를 관리함으로 위·변조 없이 해당 정보의 진위 여부만을 기록할 수 있고 특정기관에 종속되지 않고 독립적으로 운영되어 신원정보를 언제든 생성해 이용할 수 있다.

3. 대학교 개인정보 보호 현황

3.1 국내 대학교 개인정보 유출 사례

3.1.1 내부자 개인정보 유출 사례

국내 대학의 개인정보 유출 사례를 살펴보면 내부에서 교원 및 학생의 개인정보를 의도하지 않고 외부로 유출한 사례들 또한 적지 않은 것을 확인할 수 있다. [표 1]은 현재 국내 대학교들이 보관 및 관리중인 개인정보 데이터 유출 목록을 정리한 내용이다. D 대학의 경우 졸업생들의 직장까지 작성되어 있는 인명록을 제작하고 있었다 [10]. 이 인명록 같은 경우에는 온라인으로 구매할 수도 있었기에 해당 대학의 졸업생에 대한 개인정보들을 쉽게 얻을 수 있었다. H 대학 같은 경우에는 내부 직원의 실수로 해당 학교 학생의 주민등록번호까지 적힌 파일을 메일로 잘못 보낸 경우이다 [11]. K대학과 D대학 같은 경우에는 1000명 이상의 학생 개인정보가 담긴 파일을 누구나 쉽게 해당 대학의 웹사이트에서 다운로드가 가능했다 [11][12].

국내 대학의 내부자를 통한 개인정보 유출사건에 대한 유형과 사례 분석 결과 가장 중요한 문제점은 내부 유출 사례들이 모두 해당 학교의 학생들의 동의 없이 개인의 정보가 유출되었다는 것이다. 이는 내부의 실수로 인한 학생 및 교직원의 개인정보 유출을 통해서 악의적인 사람이 대학교 포털 시스템에 접속해 추가적인 개인정보나 성적 등 개인에게 민감한 정보까지도 유출을 하게 되는 2차 피해가 발생할 수 있다. 실제로 국내의 모 국립 대학교에서는 포털의 ID만을 통해서 대학교 내의 데이터베이스에 있는 주민등록번호만을 획득할 수 있고 해당 포털에 접속해 추가정인 개인의 정보를 취득할 수 있다.

[표 1] 국내 대학의 개인정보 내부 유출목록

[Table 1] List of internal leakage of personal information of domestic universities

Univ.	Leakage List	Cause	Amount(people)
D Univ. (2020)	Name, Adr, C.P, E-Mail, Company Name, Department	Directory	About 230,000
H Univ. (2019)	Name, Department, Gender, C.P, E-Mail, RRN, Trading Bank Name, Account	Staffs Accident	About 350
K Univ. (2019)	Student Id, Department, Name	Open Download	1,245
D Univ. (2017)	C.P, Student Id, Department, Tuition, Scholarship, Leave of absence	Open Download	1,321

3.1.2 외부 사이버침해의 개인정보 유출사례

대학교 내의 내부자 실수로 인한 개인정보 유출 사고는 내부의 방침과 교육을 통해서 유출행위

를 방지할 수 있지만 외부의 해킹을 통한 유출 사고는 실수가 아닌 악의적인 목적을 가지고 하는 행위이기 때문에 대학교의 보안 시스템을 통해서 개인정보 유출을 방지해야 한다. 그러나 국내의 외부적인 공격으로 인한 대학교의 서버해킹 및 개인정보 유출 사건은 빈번하게 일어나고 있다. [표 2]는 외부로부터의 공격을 통한 국내 대학교 개인정보 데이터 유출 목록을 정리한 내용이다. 국내의 D대학의 경우에는 해당 학교 학생이 포털시스템에 접속해 전산망의 취약점을 분석해서 43,413건의 학생의 개인정보를 탈취해 외부인에게 넘긴 사례가 있었고 [13], K대학 같은 경우에는 약 40,000명 이상의 학생들에게 피싱메일을 보내 학생들의 개인정보를 탈취해간 사례가 있다 [14].

국내 대학교의 개인정보 유출로 인해서 대학교의 중앙화된 서버에 개인정보를 관리하는 방식은 언제든지 유출이 될 수 있기 때문에 개인정보가 탈취될 가능성을 항상 염두에 두어야하기 때문에 국내 대학의 정보관리는 블록체인의 DID기술을 사용해 신원증명이 필요하다.

[표 2] 국내 대학의 개인정보 외부 유출목록

[Table 2] List of external leakage of personal information of domestic universities

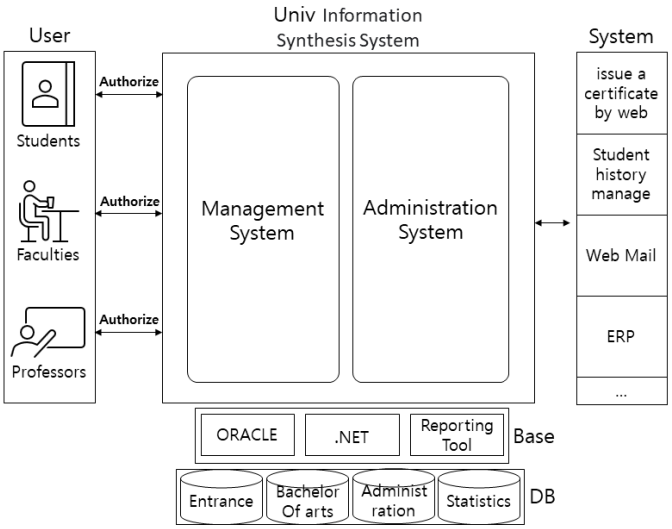
Univ.	Leakage List	Cause	Amount(people)
D Univ. (2020)	Name, ID, Password, Adr, C.P, E-Mail, Department, Grade	Vulnerability Attack	43,413
K Univ. (2019)	Name, ID, E-Mail, Department, Student ID	Fishing Mail	About 40,000

3.2 국내 대학교 종합정보 시스템 문제점

현재 국내 대학교 종합정보 관리 시스템의 구조도는 [그림 3] 과 같은 구조를 이루고 학교의 종합정보 시스템을 관리하고 있다 [15]. 학생 및 교직원들이 학교의 정보 및 서비스를 이용 받기위한 환경을 제공하기 위해 교내 웹 서버 및 웹 애플리케이션 서버를 통해 홈페이지에 로그인하여 교내 서버간의 통신을 통해 통합 DB의 각 포털 시스템에 접속해 해당 정보를 제공받고 정보를 공유하며 통합 DB에 정보가 저장된다.

국내 대학교의 내부 업무용 서버에서 중요한 웹 서버, 웹 애플리케이션 서버의 IP유형을 살펴본 결과 156개의 대학에서 131개의 대학이 모두 공인 IP로 운영을 하고 4개의 대학만이 모두 사설 IP로 관리를 진행하는 연구결과를 확인 할 수 있다 [16]. 공인 IP는 외부로부터 직접 접근이 가능한 IP이기 때문에 유출되면 매우 위험하고, 해당 IP를 통해서 취약점을 분석해 내부 서버에 있는 정보들이 탈취될 수 있다. 현재 대학은 비용 등의 문제로 정보보호 인프라가 완전하게 갖추어지지 않았고, 정보보호 관련된 전문 인력이 많이 부족해 외부에서의 공격이 이루어졌을 때 종합정보 시스템이 사이버 공격에 노출되어 학생 및 교직원의 개인정보 유출과 같은 사이버 침해가 발생할 수 있다. 국내 대학교의 사이버 침해를 막기 위해 각 서버를 영역별로 관리하거나 해당 대학에 보안 담당자를 늘리고 내부에서 보안 준수를 체계적으로 활동하는 방법도 존재하지만 본 논문은 대학교

내의 정보를 물리적 관점, 관리적 관점을 높이는 것에 중점을 둔 것이 아니라 개인이 정보를 가지고 관리함으로 대학교 종합정보 시스템에서 관리하는 시스템에서 벗어난 DID기법을 제언한다. DID기반으로 대학교의 개인정보를 관리함으로 학생 및 교직원들은 내부에서 정보를 실수로 유출하거나 외부에서 정보를 탈취당할 염려할 필요가 없다.



[그림 3] 대학 포털 종합정보시스템

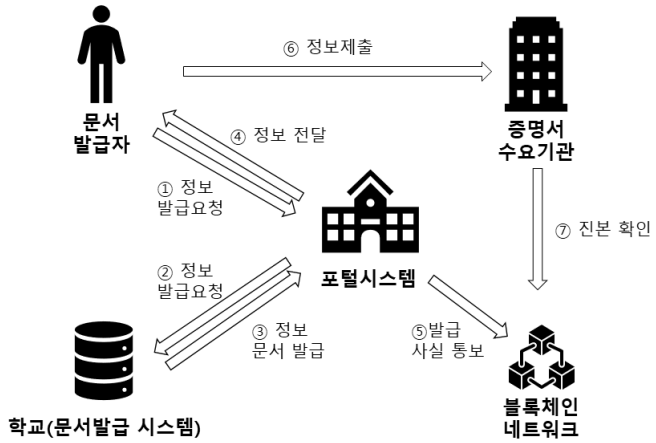
[Fig. 3] University Portal Information System

4. DID기반 대학교 학생 및 교원 개인정보 보호 및 관리 필요성

4.1 DID기반 신원증명 사용 현황 분석

국내 DID기반 자기주권신원증명 서비스를 진행하고 있는 기업들의 솔루션을 조사한 결과 대학교내의 시스템과 연관이 있는 DID기반 솔루션들은 크게 대학 제증명 서비스, ID/인증 기반 제증명 서비스 2개가 있다. 먼저, 대표적인 대학 제증명 서비스는 SK텔레콤에서 서비스 중인 Initial이다. Initial은 모바일을 통해서 나의 개인정보를 개인 단말기에 저장하고 직접 제출하는 서비스이다 [17]. [그림 4]는 initial에서 대학 제증명을 위해 DID기반으로 개발한 솔루션 구조이다. 개인이 특정 기관, 기업에 제출해야 할 대학 증명서류가 필요할 때 각 학생의 정보를 개인키를 암호화한 개인키 DB에 발급하고자 하는 사용자가 키를 요청한 후, 블록체인에 담긴 본인이 제출해야 하는 증명서류 데이터를 개인의 전자지갑에 저장한다. 개인 전자지갑에 저장한 데이터를 기관, 기업에 보내 제출하면 해당 기관 및 기업은 데이터가 위조되었거나 진본임을 확인하기 위해 해당 학교의 블록

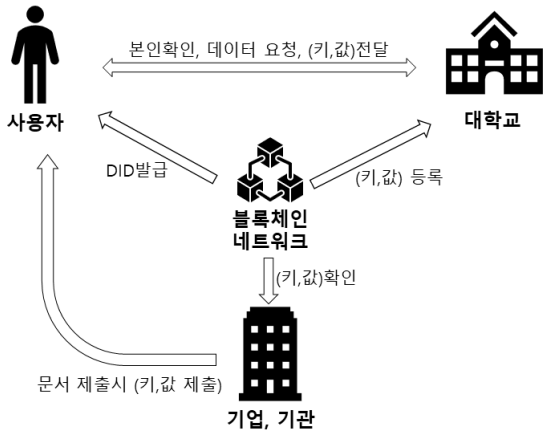
체인 네트워크에 해당 문서의 키를 조회함으로 해당 문서의 위변조를 확인할 수 있다. 국내 대학은 Initial을 통해 교직원 및 학생들이 개인정보가 담긴 학정 증명서 및 문서들을 발급받을 때 개인의 정보를 제3기관에 검증받는 것이 아니기 때문에 개인이 필요한 정보를 증명서 수요기관에 제출할 때 필요한 정보만을 직접 선택해 제출이 가능해 중간에 개인의 정보를 탈취당할 위험이 줄어든다.



[그림 4] Initial, SK텔레콤의 대학 제증명 시스템

[Fig. 4] Initial, SK Telecom's University certificate system

[그림 5]는 Coinplug의 DID를 이용한 ID/인증 기반 증명 서비스의 구조이다. ID/인증 기반 서비스는 개인정보를 사용자가 관리하는 DID기반 서비스이다 [18].



[그림 5] Coinplug DID기반 ID/인증 서비스

[Fig. 5] Coinplug ID/Authority Service based DID

대학 교원 및 교직원의 본인확인, 데이터 요청, 학생증과 같은 개인정보를 보호하기 위해서 블록체인 기반의 사용자 자신의 개인정보 및 자격 증명을 관리할 수 있도록 환경을 제공한다. 개인의 전자기기에 저장될 키, 값 데이터를 블록체인 네트워크를 통해서 발급하여 전자기기에 발급된 키를 학교에 전달해 해당 학교는 사용자에게 받은 블록체인 네트워크의 키를 통해 값을 비교하여 본인확인을 할 수 있다. 사용자의 학교와 관련된 개인정보는 모두 블록내의 Body부분에 저장되어 있으므로 이를 위변조해 사용해도 해당 블록을 통해 진위를 확인 할 수 있으므로 위변조 할 수 없고, 해당 정보에 대한 키가 개인 전자기기에 저장되므로 학교 서버를 해킹하더라도 블록에 있는 데이터는 열어볼 수 없어 개인정보 데이터를 보호할 수 있게 되고 대학 내 개인정보를 분산 관리함으로 해킹 및 데이터 유출의 리스크를 감소시킬 수 있다.

4.2 대학교의 DID기반 신원증명 효과

국내 대학이 DID기반의 탈중앙화 신원증명 기술을 이용한다면 대학과 교내 사용자들은 블록체인 상에 등록된 신원증명 데이터를 통해 제증명 발급 및 검증에 드는 비용을 최소화 할 수 있다.

4.2.1 제증명 검증절차 간소화

DID기술은 온라인상에서 문서의 위변조시 온라인에서 진본확인이 가능하기 때문에 대학의 입장에서는 현재 대학 서류 관련 부서 및 업무처의 서류관련 업무에서 증명서의 위변조 문제가 발생했을 때의 절차를 염두에 둘 필요가 없고, 해당 부서의 증명서 관련 부서 인원을 분산시켜 다른 인력으로도 사용할 수 있게 된다. 학생의 입장에서는 문서를 직접 출력하기 위한 인증서 발급 및 인증의 절차를 간소화시킬 수 있고, 인증서 비밀번호에 대한 분실 및 인증서를 공간에 대한 제약에 따른 재발급 없이 시간을 절약할 수 있다.

4.2.2 발급 및 검증 비용 절약

증명서류 절차를 간소화 시키는 것뿐만 아니라 증명서류 발급 비용 또한 절약할 수 있을 것이다. 학교는 무인증명서류발급기에 대한 유지비용을 절감하고 증명에 필요한 확인 및 인력을 절약할 수 있고, 해당 증명을 위한 물리적인 자원 또한 비용을 감소할 수 있다. 학교뿐만 아니라 학생들 또한 증명서류 출력을 위한 시간 및 자원 절약과, 현재의 인증서 비밀번호에 대한 분실 및 인증서를 공간에 대한 제약에 따른 재발급에 대한 시간을 절약할 수 있다.

4.2.3 교내 보안성 강화

현재 개인정보 유출이 많은 대학교에서는 DID를 통해서 각각의 신원 정보를 블록체인 노드에 분산시켜 저장하기 때문에 개인정보 위변조가 불가능하여 해킹 및 유출에 대한 리스크를 없애고

보안성을 높일 수 있고, 교직원 및 학생들의 정보를 개인이 관리하고 저장함으로, 내부자의 실수로 인한 유출 염려 없이 개인의 데이터 주권을 보호할 수 있다.

5. 결론 및 향후 과제

국내 대학의 개인정보에 대한 문제점은 개인정보 유출 사건이 빈번하게 발생하면서 교직원 및 학생들의 정보가 언제든지 외부로 유출 될 수 있고, 대학의 전산망 시스템이 항상 안전하지 않다는 사실이다. 따라서 본 논문은 현재까지 대학의 정보관리방식인 중앙화된 저장방식이 아니라 4차 산업혁명에 맞춰 개인의 데이터 주권을 보호하고자 개인의 데이터를 개인관리하고 배포하고자 하는 정보만 배포할 수 있도록 국내 대학의 탈중앙화된 관리방식이 왜 필요한지에 대한 이유를 분석하고 방향을 제언하였다. 하지만 아직 일부의 DID기반 서비스만이 개발 중에 있으며 호환성에 대해 극복할 문제가 많다. 때문에 국내 대학에서는 3곳 정도의 대학만이 DID기술을 사용하고 있고, 전체의 학교 시스템에서 일부분만을 DID기술을 이용하고 있으므로, 향후 DID기반의 대학교 신원관리 플랫폼 설계에 대해 자세한 연구가 뒤따라야 할 것이다.

References

[1] K. W. Bong, “Personal Information Processing and Analysis of Infringement Factors of New Technology Services in the Fourth Industrial Revolution”, Journal of Korea Institute Of Information Security And Cryptology, vol. 30, no. 5, October 2020, pp. 121-126.

[2] J. S. Park, “The research on the improvement in weakness and student information management condition of university from the view of life cycle of privacy information”, Master’s thesis, Department of Computer Engineering, Dongguk University, Republic of Korea, 2008.

[3] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system”, Bitcoin.org, https://bitcoin.org/bitcoin.pdf, (accessed January 1, 2021).

[4] Y. Akane, Block chain structure and theory, Wikibooks, 2017.

[5] E. S. Kim, “A Literature Study on Digital Currency and Historical Developments of Money: Dynamic Pattern in Currency, Central Bank Digital Currency and Libra”, The Journal of Society for e-Business Studies, vol. 25, no. 2, May 2020, pp. 109-126.

[6] J. H. Yu, “A study on Applying Privacy by Design in Block chain Services”, KISA, Seoul, Korea, Tech. Rep. KISA-WP-2019-0020, December 2019.

[7] D. Reed, M. Sporny, D. Longely, C. Allen, R. Grant, M. Sabadello, “Decentralized Identifiers(DIDs)”, W3C.com, https://www.w3.org/TR/did-core/, (accessed January 15, 2021).

[8] C. C. Group, “A Primer for Decentralized Identifiers”, W3C.com. https://w3c-ccg.github.io/did-primer/, (accessed January 15, 2021).

[9] M. Sporny, D. Longley, D. Chadwick, “Verifiable Credentials Data Model”, W3C.com https://www.w3.org/TR/vc-data-model/, (accessed January 15, 2021).

[10] Dongguk Alumni Association, Dongguk Who’s who, Dongguk Alumni Association, 2020.

[11] M. W. Yang, “Idle Status of Personal Information Protection in Universities”, boannews.com, https://www.boannews.com/media/view.asp?idx=81772, (accessed Jaunary 20, 2021).

[12] B. R. Jung, “Our university student is leaked about 1,300 perosnal information, How do we cope with our university”, dudream.daegu.ac.kr, http://dudream.daegu.ac.kr/news/articleView.html?idxno=3862, (accessed January 20, 2021).

[13] K. A. Kim, “D University, 42,361 Personal information leakage... Field of searching emergency”, boannews.com, https://www.boannews.com/media/view.asp?idx=68281&page=4&mkind=1&kind=1, (accessed Jaunary 20, 2021).

[14] J. Kwon, “KAIST, Faculty & Strudent Personal information about 30,000 leakage by hacking”, boannews.com, https://www.boannews.com/media/view.asp?idx=93154, (accessed Jaunary 20, 2021).

[15] B. T. Ahn, K. M. Park, “A Case Study on Building Integrated Portal Information System on Campus”, The Journal of Korean Institute of Information Technology, vol. 8, no. 9, September 2010, pp. 199-215.

[16] J. M. Choi, D. Y. Kim, “A Study on Security Management Methods for Information System of Educational Institutions”, The Journal of Korean Association of Computer Education, vol. 20, no. 6, November 2017, pp. 95-104.

[17] Initial, “University certificate”, initial.id, https://initial.id/html/, (accessed January 20, 2021).

[18] Coinplug, “Blockchain ID / authentication-based proof service”, coinplug.com, https://coinplug.com/kr/business#hyundaicard, (accessed January 20, 2021).