Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.6, Dec. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.6.1115

분산 ID 기반 모바일 학생증 구현과 활용*

조 승 현,[1†] 강 민 정,[1] 강 지 윤,[1] 이 지 은,[1] 이 경 현[2‡]
[1,2]부경대학교 (학생, 교수)

Implementation and Utilization of Decentralized Identity-Based Mobile Student ID*

Seung-Hyun Cho,[1†] Min-Jeong Kang,[1] Ji-Yun Kang,[1] Ji-Eun Lee,[1] Kyung-Hyune Rhee[2‡]
[1,2]Pukyong National University (Student, Professor)

요 약

본 논문에서는 이름과 학번, 학과, 안면 사진 등이 포함된 기존의 플라스틱 카드형 학생증에서 자기 주권 신원(Self Sovereignty Identity, SSI)을 보장하기 위한 모바일 학생증을 구현하였다. 구현된 모바일 학생증은 플라스틱 학생증을 분실하여 신원이 노출되는 문제점을 해결하고 스마트폰 단말기에서 애플리케이션을 통한 전자 학생증으로 편의성에 특화된 블록체인의 분산 ID(Decentralized Identity, DID) 기반으로 개발된 FRANCHISE 모델의 구조와 프로세스를 갖추고 있다. 또한, 개인에 의한 개인정보 제어로 안전성을 보장하며, 스마트폰을 이용함으로써 편리하게 학생의 신분을 증명할 뿐만 아니라 교내 행사 참여, 온라인 인증, 다른 학교 간의 교류 등 다양한 서비스 확장이 가능할 것으로 기대된다.

ABSTRACT

In this paper, we developed a mobile student ID providing a self sovereignty identity (SSI) which replaces the conventional plastic-type student ID that includes private information of a student such as a name, a student number, a facial photo, etc. The implemented mobile student ID solves the problem of exposing student's identity due to a loss or a theft of a plastic-type student ID, and it has a structure and process of FRANCHISE model which is developed by a concept of a decentralized Identity(DID) of a Blockchain, in which specialized for convenience as an electronic student ID through an application on a smart phone device. In addition, it protects student's privacy by controlling personal information on oneself. By using a smartphone, not only it easily identifies the student but also it expands to several services such as participation in school events, online authentication, and a student's exchange program among colleges.

Keywords: Blockchain, Decentralized Identifier, ID Authentication

I. 서 론

오늘날 디지털 기반인 신원증명 시스템은 서비스 제공 업체들 사이에 단편화되어 있다. 사용자는 서비스 간에 자신의 신원정보를 복제할 필요가 있으며, 이로 인해 전체적인 사용성이 저하되고 데이터 손상

Received(09. 29. 2021), Modified(11. 16. 2021), Accepted(11. 16. 2021)
* 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2021-2020-0-01797) 일부는 2019학년도 부경대학교 연구년 교수 지원사업에 의하여 연구되었음 (C-D-2019-0318)
* 본 논문은 2021년도 한국정보보호학회 하계학술대회에 발표한 우수논문을 개선 및 확장한 것임
† 주저자, netkingj@gmail.com
‡ 교신저자, khrhee@pknu.ac.kr(Corresponding author)

의 위험이 증가한다. 개인정보를 관리하기 위해 중앙 집중화된 기업을 신뢰하는 것은 데이터 유출, 사생활 침해, 신원 도용과 같은 개인정보 침해 문제를 일으킬 수 있다. 자기 주권 신원(self-sovereign identity, SSI)은 개인에 의해 자주적인 데이터 제어와 투명성이 유지되도록 하는 신원 관리에 대한 사용자 중심 접근 방식이다. 또한, 끊임없이 증가하는 중앙집중화된 기업의 구조적 문제로부터 사용자의 권리를 보호하고, 개인정보와 관련된 서비스와의 정보 이동, 호환이 가능하도록 도움을 주는 역할을 한다.

블록체인 기반 자기 주권 신원증명 모델을 적용하면, 기존 신원증명 시스템의 문제를 해결할 수 있다. 대학교의 경우, 학생 신분 인증을 위해 학생증이 이용되며 학생 신분을 증명하는 용도로 도서관 출입, 온라인 대학 커뮤니티 학교 인증 등으로 사용되고 있지만, 불필요한 정보들(얼굴, 신용카드 번호 등)까지도 함께 제시함으로써, 개인정보가 지나치게 노출되고 플라스틱 카드를 늘 소지해야 하는 불편함 또한 존재한다.

본 논문에서는 스마트폰이 대중화된 시대에 학생증을 디지털 형태로 소지할 수 있도록 고안해 필요한 정보를 선택적으로 제시할 수 있게 하여, 사용자들의 개인정보 공개를 최소화로 보호하고, 편리성을 높일 수 있다는 장점으로 분산 ID 기반 모바일 학생증을 구현하여 활용 방안을 제시한다. 또한, 분산 ID 관련 연구 사례 조사를 진행하면서 기존에 제안된 모바일 학생증을 분석하여 본 모델이 지닌 장점을 제안하고, 기존에 제시한 서비스 모델과는 다르게 W3C에 따른 표준 보안 요구사항 체크리스트를 제시하여 안전성을 분석한 확장된 FRANCHISE 모델을 제시하고자 한다[1].

II. 관련 연구

기존의 중앙 서버에 정보 주체 개인의 데이터가 모두 모여 있는 인증 방식과는 달리 분산 ID는 개인이 직접 자격 증명을 발급받아 신원정보와 함께 모바일 단말기 등에 보관하고 필요할 때마다 선택적으로 신원정보를 제출하는 인증 방식이다. 또한, 이러한 분산 ID 기술을 이용한다면 국경을 넘는 인증이 가능하다. 이처럼 분산 ID 기술을 통해 얻을 수 있는 이점들로 인해 현재 국내에서는 분산 ID에 관한 연구가 활발히 진행되고 있으며, 그에 대한 기술력을 높이려 노력하고 있다.

2.1 국내 사례

2.1.1 COOV 애플리케이션

질병관리청이 분산 ID 기술을 활용하여 개발한 COOV 애플리케이션은 사용자의 개인정보를 저장·관리하고, 분산 ID가 포함된 QR code를 스캔하여 사용자 본인임을 증명하는 방식의 백신 여권 애플리케이션이다. 이를 통해 질병관리청에서 COVID-19 예방접종서를 내려받아 스마트폰에 저장하여 QR code를 통해 사용자 본인임을 증명하고 싶을 때 언제든지 기관에 제출할 수 있으며 원하는 개인정보만 선택할 수 있어 불필요한 개인정보를 노출에 방지한다[5].

2.1.2 PASS 애플리케이션

PASS 애플리케이션은 이동통신사 3사(SK텔레콤·LG유플러스·KT)가 제공하는 인증 앱이며, 분산 ID 기술을 활용했다. 스마트폰으로 본인 인증을 하고 나면 그 뒤에는 필요할 때마다 추가적인 확인 절차 없이 본인 인증 시 등록해놓은 패스워드를 입력 후 인증서 발급이 가능하다. 기존 출시된 또 다른 인증 애플리케이션들보다 간편한 방식으로 사용자들의 편익을 높였다. 이외에도 본인 인증서뿐만 아니라 모바일 운전면허증, QR code 출입증, 백신 접종 인증 등의 다양한 인증 서비스를 제공한다[6].

2.1.3 Initial 애플리케이션

SKT에서 블록체인 분산 ID 기술을 접목해 출시한 Initial 애플리케이션은 사용자가 본인의 스마트폰 단말기에 다양한 증명서를 발급하여 저장한 후 제출하도록 도와주는 서비스 애플리케이션이다. 행정안전부가 운영 중인 정부24 서비스와 연동하여 공공증명서 발급 서비스를 시작했다. 이전에는 업무처리를 위해 각종 신청서 및 구비서류 등을 팩스 또는 이메일로 제출하거나 직접 방문해야 했지만, Initial을 통해 직접 방문하는 수고 없이도 서류 제출이 가능하므로 더욱 간편하다는 특징을 지닌다[7].

2.1.4 MYKEEPiN 애플리케이션

MYKEEPiN 애플리케이션은 블록체인 기술 기

업 중 하나인 코인플러그가 분산 ID 기술을 활용하여 개발한 디지털 확인 증표 애플리케이션이다. 이전에는 디지털 본인 확인 증표를 처음 발급하기 위해 영상통화로 실명 확인 증표와 대조했는데, MYKEEPiN은 영상통화 없이 실명 확인 증표의 사진과 얼굴 촬영 화면을 대조하는 안면인식 기술 활용하여 영상통화 없이도 디지털 본인 확인 증표를 발급할 수 있게 하는 것을 가능하게 했다. 이후 실명 확인을 할 때는 고객 스마트폰에 발급·저장된 디지털 실명 확인 증표를 제시하면 실명 확인이 손쉽게 완료된다. 이를 통해 스마트폰 인증, 이메일 인증, 무인 편의점 출입 인증, 나이 확인 인증, 비대면 서비스 인증, 가상자산 본인 확인 인증 등의 서비스를 제공한다[8].

2.1.5 B PASS 애플리케이션

2020년 부산광역시에서 분산 ID 기술을 활용한 신원증명 서비스 애플리케이션을 출시했다. 정부24에서 발급받은 주민등록표등본과 건강보험 자격확인서 등의 전자 증명서 100종을 B PASS 애플리케이션으로 열람하거나 필요한 곳에 제출할 수 있다. 해당 서비스를 이용하기 위해 처음에만 본인 인증하고 나서 분산 ID가 포함된 QR code 신분증을 발급받을 수 있다. 이를 통해 필요한 증명서를 사용자가 용도에 맞는 곳에 제출할 수 있다[9].

2.1.6 KU 모바일 ID

고려대학교는 국내 대학 최초로 분산 ID 시스템을 도입하여 모바일 학생증인 KU 모바일 ID 애플리케이션을 개발했다. 이는 본래 운영 중이던 스마트카드 학생증 발급 시스템과 모바일 학생증 발급 데이터베이스를 연동하여 학생임을 검증하고 개인화된 ID를 각각의 모바일 기기에 발급해주는 형태로 이루어진다. 이를 통해 플라스틱 학생증 없이도 모바일 ID가 저장된 스마트폰만 있다면 교내 신원확인이 가능하도록 했다[14].

2.1.7 Eduwallet

Eduwallet 애플리케이션은 초중고 학생들을 대상으로 하여 에듀블록플랫폼(주)에서 개발한 전자지갑 애플리케이션이다. 학생은 먼저 학교에 승인 신청 후 분산 ID가 포함된 QR code를 발급받을 수 있다. 대부분의 초중고 학생들에 대한 정보가 국가 법령에 따라 NEIS에 기록되고 저장되어있는 것과 달리 해당 애플리케이션은 전자지갑 내에 자신의 정보를 기록하고 저장하는 것이 가능하도록 했다. 또한, 학생증뿐만 아닌 표창장 등 각종 증명서 등을 저장할 수 있는 기능을 추가할 예정이다[15].

2.2 해외 사례

2.2.1 Verified.Me 애플리케이션

캐나다 은행들은 블록체인 기반 신원 인증 서비스인 Verified.Me 애플리케이션으로 사용자들의 신원을 인증하여 더욱 간편하게 금융 서비스를 이용할 수 있도록 블록체인 네트워크를 공동으로 운영하고 있다. 이를 통해 사용자는 각각의 은행마다 신원 확인 과정을 반복해 거칠 필요 없이 해당 애플리케이션에 등록된 모바일 신분증을 이용하여 은행별 서비스를 이용할 수 있다[11].

2.2.2 Shocard ID Wallet 애플리케이션

미국의 벤처기업 ShoCard에서는 블록체인 기반의 모바일 신원증명 서비스인 ShoCard ID Wallet 애플리케이션 제공하고 있다. 이는 사용자가 애플리케이션을 설치하고 나서 분산 ID 발급하기 위해 신분증에서 개인정보를 암호화하여 모바일 내 저장하는 방식이다. 또한, 사용자가 서비스 이용 시 필요한 신원정보를 선택하여 제시할 수 있다[12].

III. 보안 요구사항

3.1 W3C 보안 요구사항 체크리스트

다음은 W3C에 따른 분산 ID 보안 요구사항 체크리스트로 Table 1.와 같이 제시한다[2][3].

1) 분산(Decentralized)

분산 ID는 중앙 서버에서 사용자의 신원정보를 관리하지 않음으로 서버의 갑작스러운 중지로 인한 사용자 정보 유실 혹은 해킹 등의 공격으로 인한 사용자 정보 유출 등과 같은 외부 환경 변화와 관련된 문제가 일어날 확률이 낮다. 그러므로 보안 측면에서

의 장점을 높이기 위해 중앙 발행기관 없이 사용자의 신원정보와 검증 정보를 블록체인 네트워크상에 기록하여 탈중앙화 신원증명을 보장하여야 한다.

2) 무결성(Integrity)

분산 ID는 본인 인증 그리고 데이터의 무결성 보호 및 제공이 필요하다. 예를 들어, 무결성을 보장하는 방법의 하나로 트랜잭션(Transaction)의 암호키 생성을 이용하면 트랜잭션 정보를 안전하게 암·복호화하여 외부로부터의 공격으로 인한 사용자 정보 유출을 예방할 수 있고 트랜잭션 내용의 위·변조를 방지할 수 있다. 이처럼 데이터의 무결성을 제공하여 보안 문제를 해결하는 방법에 대한 고려가 필요하다.

3) 기밀성(Confidentiality)

개인정보에 관한 암호화 방식 그리고 사용자가 자신의 개인정보에 접근하는 방법과 같은 기밀성을 제공하기 위한 사용자의 데이터에 관한 보안 메커니즘(Mechanism)에 대한 고려가 필요하다.

4) 인증(Authentication)

기기 인증 및 본인 인증 과정 중 도청 또는 중간자 공격 등의 인증 시 발생할 수 있는 취약한 공격에 대응할 방법에 대한 고려가 필요하다.

5) 가용성(Availability)

어떤 방식으로 허용된 사람만 데이터에 대한 접근이 가능하게 할 것인지, 어떤 방식으로 여러 사용자가 동시에 자신들의 개인정보에 접근할 때를 관리해야 네트워크에 장애가 발생하지 않을 것인지 대한 고려가 필요하다.

3.2 W3C 분산 ID 개념 및 표기 방법

W3C에서 분산 ID는 검증할 수 있고 탈중앙화된 디지털 신원을 위한 새로운 형식의 식별자로, 분산 ID 컨트롤러가 분산 ID의 제어권을 증명하고, 중앙화된 레지스트리(Registry), 신원 제공자, 인증기관 등으로부터 독립적으로 구현할 수 있도록 설계되었다.

분산 ID 표기 방법은 URN(Unified Resource Name) 규격 참고하여 Fig. 1.와 같이 세 부분의 문자열로 구성되어 있다.

1) URL Scheme Identifier (DID) : 분산 ID 주체를 식별하는 것으로 'did'로 시작한다.

2) Identifier for the DID method : 특정 분산 ID 체계가 특정 분산원장이나 네트워크에서 구현할 수 있는지에 대한 정확한 방법을 정의한 것으로, 메소드 이름은 5자 이하여야 한다.

3) DID Method Specific Identifier : 해당 분산원장에서 분산 ID가 저장된 실제 주소이다. 중앙화된 레지스트리 서비스를 이용하지 않고 생성할 수 있어야 하고, 범용(범세계)적으로 고유해야 한다.

Fig. 1. A simple example of a decentralized identifier(DID)

Table 1. W3C Security Checklist

No.	Requirements	Checklist
1	Decentralized	· There should be no central issuing agency
2	Integrity	· Data · Device authentication · Identification verification
3	Confidentiality	· Encryption (How to protect data) · Device authentication · Control access to data · Identification verification · Which part of data is protected
4	Authentication	· Device authentication (password setting) · Vulnerable types of authentication attacks
5	Availability	· Access control design

3.3 W3C 분산 ID 상호운용성

분산 ID의 구현 상호운용성은 규격에 부합하는 분산 ID를 작성하고 분석할 수 있는 구현 능력을 평가하여 시험한다. 분산 ID Method의 상호운용성은 최소한 다음과 같이 규격을 평가함으로써 결정된다.

- 분산 ID Method 이름은 겹치지 않고 유일해야 하며, 분산 ID Method의 기존용례와 모순된 사용은 하지 못함.
- 요구되는 기능 지원.
- 설명이 필요한 작업에 관한 설명이 필요.
- 규격은 독립적 구현을 위해 충분히 구체적이고 상세하고 완전해야 함.
- 규격은 Security 및 Privacy 고려사항을 기술하는 Section을 포함해야 함.

분산 ID의 생산자와 소비자를 위한 상호운용성은 분산 ID가 일치하는지 확인함으로써 보장된다. 그리고 상호운용성을 높이기 위해, 분산 ID 정규화는 가능한 보편적이고 간단해야 한다.

- 분산 ID 스키마는 무조건 소문자.
- 분산 ID Method 이름은 무조건 소문자.
- 분산 ID 구문의 method-specific-id 규칙의 값의 대소문자 구분과 정규화는 관리되고 있는 분산 ID Method에서 무조건 정의되어야 함.

IV. 시스템 모델

4.1 시스템 모델 개요

Fig. 2.과 같이 분산 ID 기반 모바일 학생증 FRANCHISE 모델의 전체적인 구조는 자체 구현한 Golang 기반의 블록체인 네트워크 FRANCHISE, 학생 정보와 분산 ID 문서를 저장·관리하는 데이터베이스인 MariaDB, 안드로이드와 FRANCHISE의 통신을 위한 게이트웨이 gRPC, 인증 서비스 제공을 위한 Rasberry Pi와 학교 이메일 그리고 안드로이드 가상 단말기 임무를 수행하는 에뮬레이터 실행을 위한 IntelliJ IDEA로 이루어져 있다. 안드로이드와 분산 ID 문서가 저장되어 있는 FRANCHISE는 gRPC를 게이트웨이로 하여 서로 정보를 주고받는다. 이 과정에서 FRANCHISE 서버에서 이용자인 학생이 본 학교 학생인지 학교 이메일 계정을 통해 인증하는 작업과

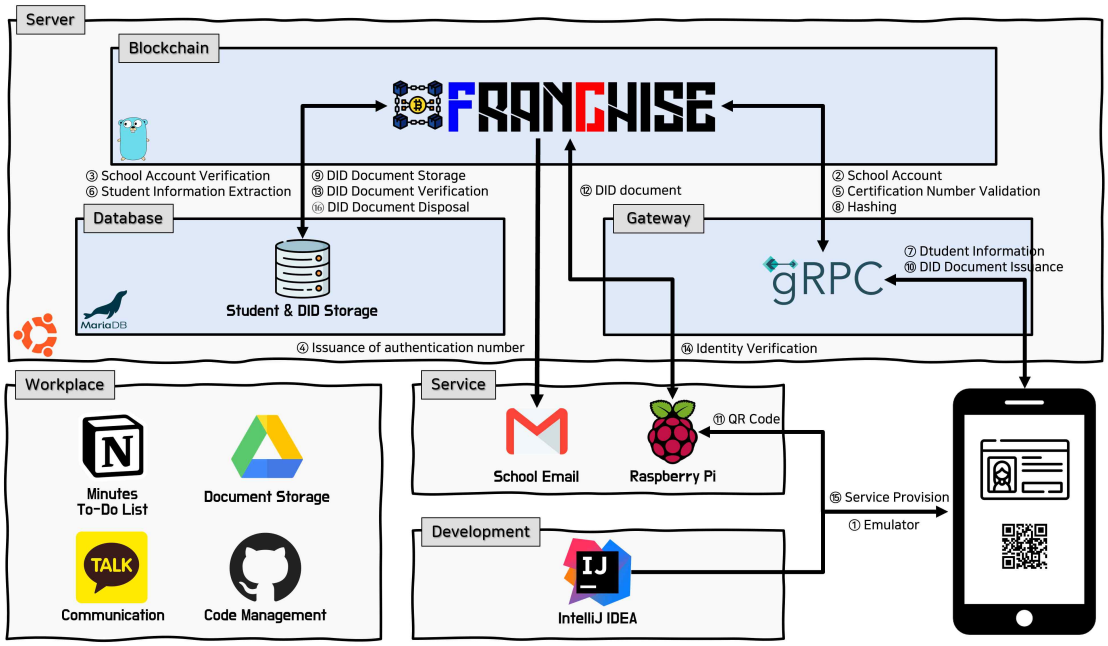

Fig. 2. Project Architecture(1)

학생 정보를 통해 분산 ID 문서를 생성하여 안드로이드에게 전달해주는 작업 등이 이루어진다. 안드로이드에서는 FRANCHISE에서 받은 분산 ID 문서 정보를 이용하여 QR code를 생성한다. 이렇게 생성된 QR code를 스캔하여 검증 기관에서 신원 인증 시 활용된다.

4.2 시스템 모델 구조

Fig. 3.와 같이 FRANCHISE 모델을 이용한 분산 ID 기반 모바일 학생증 구조는 크게 네 부분으로 이루어져 있으며 사용자, 발행기관, 검증 기관 그리고 블록체인으로 구성되어 있다. 사용자는 Application을 이용하여 발행기관의 분산 ID 문서 발급, 검증 기관의 분산 ID 문서 검증과 같은 분산 ID 정보의 접근 제어를 수행하며 발급과정에서 개인키를 저장한다. 발행기관은 서버를 통해 Application에서 이메일 계정을 전달받아 사용자의 신원을 조회한 후 신원 인증이 완료되면 학생 정보를 Application에 전달하고 Application에서 학생 정보와 개인 키를 합한 해시값과 함께 분산 ID 정보 발행 요청을 함으로써 사용자에게 분산 ID 문서를 발급하여 준다. 또한, 블록체인은 앞 과정에서 얻은 분산 ID 정보를 등록하며, 저장된 분산 ID 해시값을 통해 사용자에게 서비스를 제공해주는 검증 기관에 인증이 필요할 때마다 검증을 진행한다.

4.3 시스템 모델 프로세스

Fig. 4.와 같이 분산 ID 기반 모바일 학생증에 보안과 편의성이 강화된 FRANCHISE 모델의 시스템 프로세스는 총 4단계로 신원 조회, 분산 ID 문서 생성 및 발급, 신원 검증 그리고 만료 단계로 이루어져 있다.

4.3.1 신원 조회

분산 ID 문서 생성 및 발급은 학생의 정보와 개인 키를 활용해 분산 ID 문서로 생성하여 학생에게 발급하는 단계이다.

① 학생은 자신의 스마트폰에 애플리케이션을 설치한 뒤, ② 신원을 조회하기 위해 학교 도메인으로 등록된 이메일 계정을 입력한다. ③ FRANCHISE

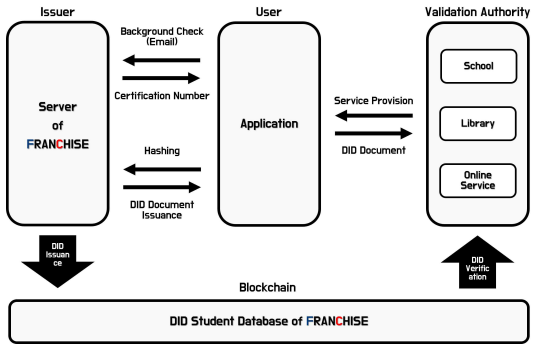

Fig. 3. System Model

는 학생으로부터 받아온 학교 계정을 검증하기 위해 학생 정보가 담긴 데이터베이스를 통해 계정 존재 여부를 파악하여 ④ 해당 계정으로 문자와 숫자가 무작위로 혼합된 인증 번호를 발급하여 전달한다. ⑤ 학생은 자신의 수신된 메일함에서 인증 번호를 가져와 애플리케이션에 입력하여 FRANCHISE에게 검증을 받음으로써 신원이 조회된다.

4.3.2 분산 ID 문서 생성 및 발급

분산 ID 문서 생성 및 발급은 학생의 정보와 개인 키를 활용해 분산 ID 문서로 생성하여 학생에게 발급하는 단계이다.

⑥ 학교 데이터베이스에서 학생 정보인 학과, 학번, 이름, 이메일 그리고 학교 코드를 FRANCHISE 통해 ⑦ 애플리케이션으로 전달된다. ⑧ 가져온 학생 정보와 임의로 생성한 개인 키(패스워드)를 256bit로 구성된 SHA(Secure Hash Algorithm) 알고리즘인 SHA-256으로 해시를 생성하여 FRANCHISE로 전달하고, 이는 평문 데이터를 알아내기 위한 복호화가 거의 불가능하여 트랜잭션의 무결성이 보장되어 신원 검증이 가능하다. ⑨ 애플리케이션에서 받은 해시값은 Fig. 1.와 같이 분산 ID 문서 형태로 변환하여 데이터베이스에 저장하고[2] ⑩ FRANCHISE는 애플리케이션으로 분산 ID 문서를 전달받은 뒤 QR code 형태로 변환하여 애플리케이션 화면에 출력한다. 또한, 재발급 시, Fig. 5.와 같이 설정 화면에서 필수 정보인 사용자가 재학 중인 대학교 이름, 학번을 제외하고 성명, 학과, 이메일, 생년월일인 선택정보를 QR code에 추가할 수 있다.

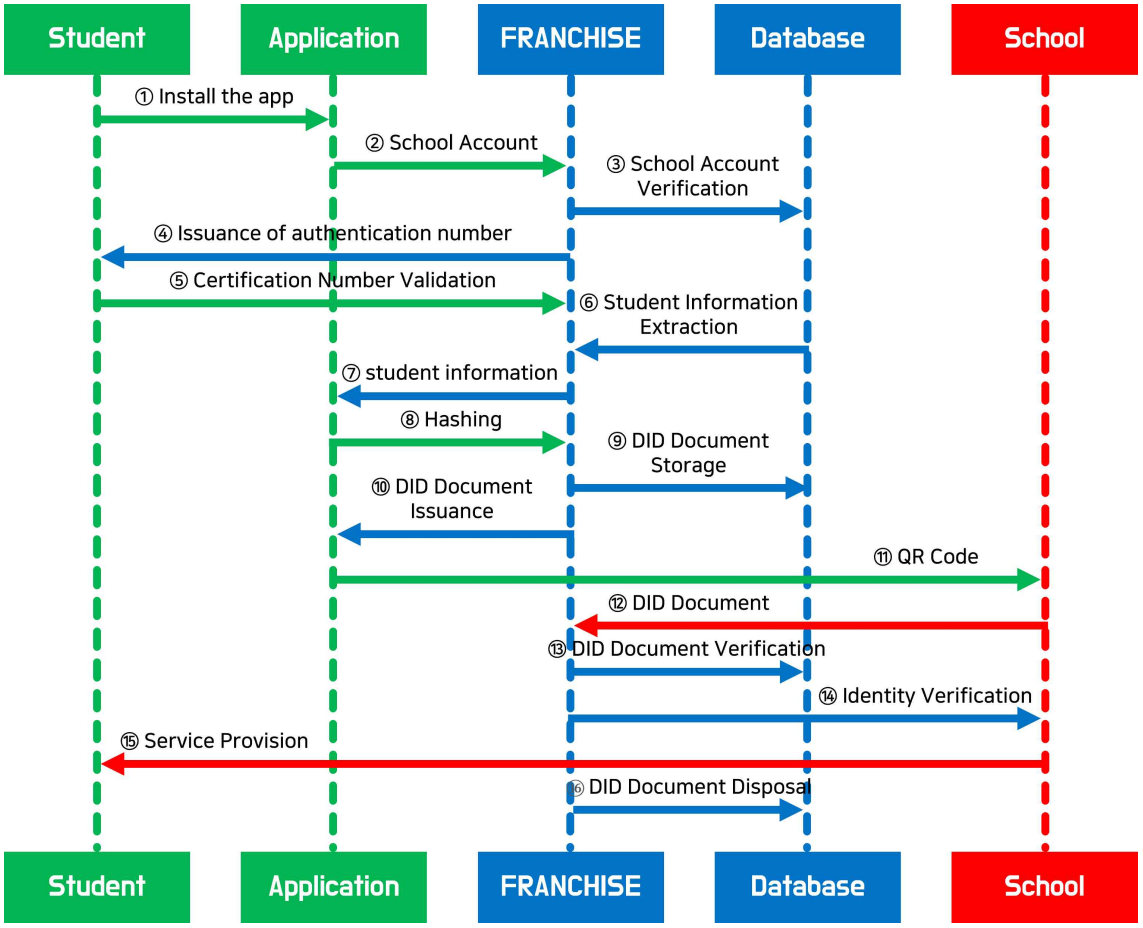

Fig. 4. System Processes

4.3.3 신원 검증

신원 검증은 검증 기관인 학교 내에 도서관, 강의실 그리고 연구실처럼 일반 학생이나 관계인이 출입할 수 있도록 신원을 검증하는 단계이다.

⑪ 학생은 신원을 검증하기 위해 Fig. 6.와 같이 애플리케이션에 본인 인증 시 생성된 해시값인 발급된 QR code로 변환된 분산 ID 문서를 검증기관의 QR code 인식이 가능한 단말기에 제시하여 분산 ID 문서를 전달하여 ⑫ 전달받은 검증 기관은 학생의 분산 ID 문서를 검증하기 위해 FRANCHISE로 분산 ID 문서를 다시 전달한다. ⑬ FRANCHISE는 전달받은 분산 ID 문서를 분산 ID 데이터베이스를 통해 Hash 값을 비교하며 검증한다. ⑭ 검증이 완료되면, 검증 기관에 검증 성공이면 성공 메시지와 함께 학생 정보를 학생 데이터베이스에서 데이터를 추출하여 전달하고 실패일 때 실패 메시지를 전달하고 ⑮ 검증 결과 성공일 때 서비스인 출입을 허가하거나 신원 파악 혹은 수집이 진행된다.

4.3.4 만료

만료는 분산 ID 문서를 통해 신원 검증이 이뤄지는데 이때 신원을 구분하기 위한 ID 값인 해시값이 유출된다면 임의로 위장 신분이 가능하여 특정 시간(수초에서 수분까지)을 두고 해시값을 변경함으로써 문제점에 대응하기 위한 단계이다.

⑯ 공격자로부터 분산 ID 문서를 가로채어 위장 신분의 문제점에 대응하고자 FRANCHISE뿐만 아니라 애플리케이션에서도 특정 시간 이후 해시값이

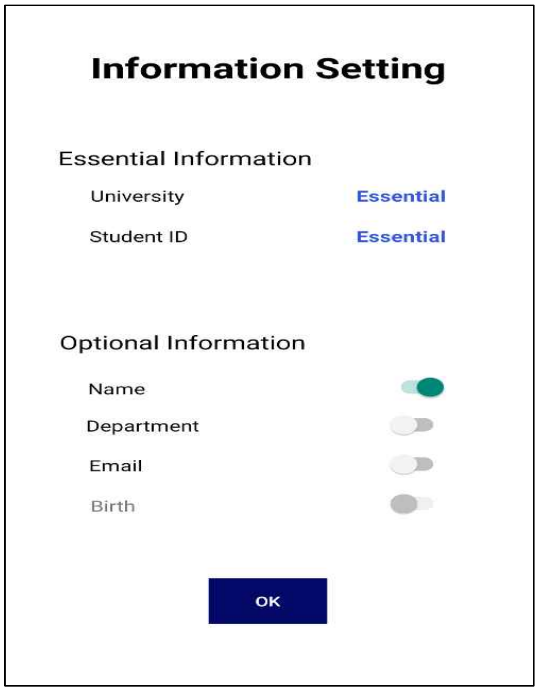

Fig. 5. Mobile App Interface for Information Delivery Settings

Fig. 6. Mobile App Interface for Decentralized ID converted to QR code

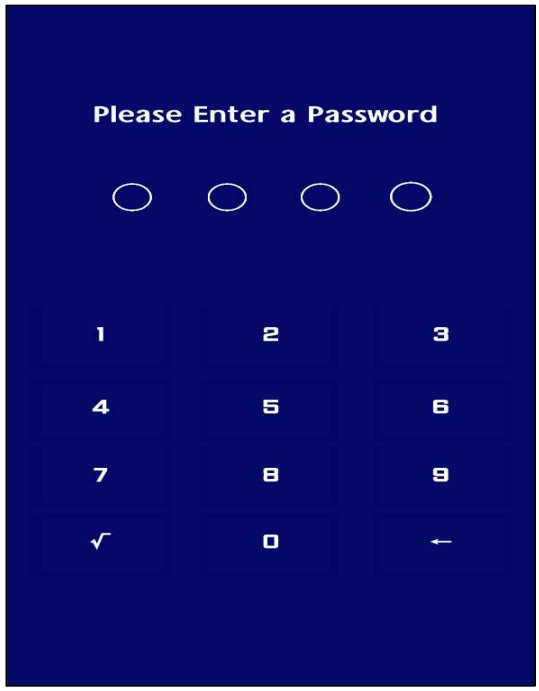

Fig. 7. Mobile App Interface for Update Decentralized ID Document

변경되므로 학생은 신원 검증을 위해 다시 발급해야 한다. 분산 ID 문서에서 ID 값인 해시값이 폐기되고 재발급 시에는 ⑧의 과정부터 다시 Fig. 7.와 같이 애플리케이션에서 생성한 개인 키를 FRANCHISE의 분산 ID 문서에서 개인 키를 비교하여 본인인증 후 FRANCHISE로 해시값을 전달함으로써 분산 ID 문서를 갱신한다.

V. 보안 요구사항 평가

5.1 제안 모델의 안전성 분석

3장에서 언급한 분산 ID의 W3C 표준 보안 요구사항을 통해 도청(Wiretapping), 재생(Replay), 메시지 삽입(Message Insertion), 삭제(Deletion), 수정(Modification) 그리고 중간자 공격(Man-in-the-middle, MITM)으로부터 대응하고 잠재적인 서비스 거부 공격(DoS) 식별과 프로토콜에 암호화 보호 메커니즘이 통합된 경우 무조건 보호되는 데이터 부분과 보호 대상이 명확하게 표시되어야 하고 암호학적 보호가 어떤 종류의 공격에 취약한지와 비밀로 유지해야 하는 데이터는 명확하게

표시했는지 만일 본 기술에 인증과 사용자-호스트 간 인증이 포함된 경우 무조건 인증 방법의 보안을 명확하게 명시하는 것에 대해 여기서는 제안 모델의 안전성 분석을 기술한다[4].

1) 분산(Decentralized)

검증 기관은 학생이 제출한 신원정보를 검증해 신원정보를 발급하고, 개인의 신원정보 발급 관련 검증 정보를 블록체인에 기록하여 탈중앙화 신원증명을 보장한다.

2) 무결성(Integrity)

학생의 신원정보는 256bit로 구성된 SHA 알고리즘인 SHA-256 Hash 연산으로 평문 데이터를 복구할 수 없어서 본인 인증 시 생성된 Hash 값인 QR code를 검증 기관에 제시하기 때문에 트랜잭션(Transaction)의 공유와 공개에 따른 트랜잭션의 무결성 위협에 대한 보안 문제를 해결한다.

3) 기밀성(Confidentiality)

대학에서 블록체인을 학생증에 활용하기 위해서는 학생의 중요 정보와 개인정보에 대해서 기밀성을 제공할 수 있는 보안 메커니즘이 필요하다. FRANCHISE는 미리 등록된 학교 도메인 계정으로 신원 인증을 진행하기 때문에 학생의 계정이 탈취되는 시나리오가 아닌 이상 FRANCHISE API를 사용하는 위장(Invalid) 애플리케이션이라도 임의로 개인 키를 발급할 수 없다. 또한, FRANCHISE의 Smart Contract, Commitment Scheme을 이용한 사설 블록체인 기반 암호화 프로토콜의 응용 모델을 구현하여 기밀성을 보장한다[13].

4) 인증(Authentication)

애플리케이션으로부터 QR code로 변환된 학생의 분산 ID 문서를 FRANCHISE 서버에 저장된 학생의 해시값과 비교 검증하여 신원 인증이 이루어진다. 이때, 애플리케이션으로부터 생성된 QR code에 저장된 학생 분산 ID를 FRANCHISE 서버에 저장된 해시값과 비교 검증하는 통신 과정에서 중간자가 침입하여 네트워크 통신을 조작하여 QR code를 빼앗아 가는 데이터 도청, 중간자 공격 등 인증 시 취약한 공격이 발생할 수 있다. 이와 같은 공격을 예방하기 위해 FRANCHISE는 일정 시간이 지나면 이전 애플리케이션에서 만들었던 것과 같은 QR code로 인증할 수 없도록 인증 시 비교 검증에 사용되는 FRANCHISE 서버의 해시값을 일정 시간이 흐른 후 폐기하고 다시 인증하기 위해 애플리케이션에서 패스워드를 입력하도록 하였다.

5) 가용성(Availability)

학생 분산 ID 문서를 발급하기 위해서는 반드시 개인 키가 필요하며 이외에는 분산 데이터베이스로 같은 정보가 담긴 블록체인이 각각의 네트워크 참가자들에 의해 분산되어 저장 및 관리되므로 장애가 발생하더라도 가용성에 문제가 발생하지 않는다.

5.2 기존 모델과의 비교분석

본 절에서는 제안한 분산 ID 기반 시스템과 2장에서 살펴본 COOV 애플리케이션, Initial 애플리케이션, MYKEEPiN 애플리케이션, Verified.Me 애플리케이션, Shocard ID Wallet 애플리케이션을 비교 분석하여 Table 2.같이 10개의 항목에 대한 제안 모델을 평가한 결과이다.

Representative Case는 해당 모델을 사용한 대표 사례를 나타내며, Working Mechanism은 작동 메커니즘, Consensus Algorithm은 합의 알고리즘 종류, Byzantine Fault Tolerance는 비잔틴 장애 허용 여부, Network Type은 네트워크 형태, Cryptocurrency는 암호 화폐 여부, Monetary Value는 화폐의 가치, Transaction Anonymity는 거래상 익명성이 가능한지, Key Features는 주요 특징을 나타낸다. 실험 결과에서 신뢰 기간인 정부・지자체・공공기관 등에서 주로 사용되는 COOV 애플리케이션을 이용하였을 때 가장 분산 ID 목적에 맞는 최적의 결과를 보였다. 이는 Public Blockchain과 Private Blockchain의 합의 알고리즘에 대하여 PoW와 RAFT가 아닌 PoT-aBFT(Proof-of-Transaction asynchronous BFT) 방식으로 선출된 블록 생성자들과 미리 지정된 신뢰 노드들을 포함하여 신뢰 기관을 중심으로 구축하는 블록체인 네트워크의 경우 미리 지정된 신뢰 노드들을 추가하여 네트워크의 안정성과 신뢰성이 높았기 때문에 제안한 모델과 다른 애플리케이션보다 최적화된 모델로 해석했다. 또한, 2장에서 언급한 기존 분산 ID 모바일 학생증 애플리케이션인 KU 모바일 ID, Eduwallet과는 달리 학생증 발급 시 학번, 이름 그리고 학생 사진 등 모든

Table 2. Comparative analysis with existing models[5][7][8][10][11][12]

	Blockchain-based Applications					
	FRAN CHISE	Initial	MYKEEPiN	COOV	Verified.Me	Shocard ID Wallet
Representative Case	FRAN CHISE	Initial	NFT	Infra Blockchian	Verified.Me	Shocard ID Wallet
Working Mechanism	University	Consortium	Consortium	Trusted Authority	Trusted Authority	Enterprise
Consensus Algorithm	PoW	-	dPKI	PoT-aBFT	-	-
Byzantine Generals Problem	○	○	○	○	○	○
Network Type	Flexible	-	Flexible	Flexible	Flexible	Flexible
Cryptocurrency	×	○	○	×	○	×
Monetary Value	×	-	-	LoW Volatility	-	-
Transaction Anonymity	○	○	○	○	○	○
Key Features	Easy Student Certification	Unlisted stock market platform	2 Factor Authenticatio n	Stable Token	Hybrid Approach	Secure Identification

정보를 한 번에 제시하지 않고 신원 인증에 필요한 정보를 선택할 수 있다. 이를 통해 QR code로 발급된 분산 ID 문서를 가지고 신원 인증이 가능하다는 점에서 기존 모바일 학생증 모델과 비교해보았을 때 개인 정보 관리가 더 뛰어나다.

VI. 결 론

기존의 신원증명시스템은 대부분 중앙 집중화된 기관들로 이루어져 있어 예상치 못한 공격에 방어하지 못하면 보안에 문제가 생길 수 있고 사용자가 자신의 신원정보를 복제하면서 데이터 손상이 발생할 수 있다. 하지만 블록체인을 기반으로 하는 분산 ID를 적용하면 기존 문제점을 보완하고 블록체인을 토대로 신뢰 된 ID 저장소를 이용하므로 분산원장에 참여한 사용자 누구나 개인정보의 위·변조 여부를 파악할 수 있다. 또한, 사용자가 자신의 신원정보 사용 및 목적을 스스로 결정할 수 있어 개인이 데이터를 제어할 수 있고 저장소의 투명성을 높일 수 있다. 본 논문에서는 자기 주권 신원(Self-sovereign Identity, SSI)을 보장하기 위해 이전에 제안한 분산 ID 기반 모바일 학생증 모델을 통해 프로세스를 검증하였고, 실제 구현을 통해 고객층의 범위를 학생으로 축소하여 학생만을 위한 유일한 서비스를 제공한다. 또한, 분산 ID의 W3C 표준 보안 요구사항 분석을 통해 해당 모델의 안정성 분석과 기존의 분산 ID 모델과의 비교분석을 통해 중앙집중화된 시스템의 문제점을 해결한 분산 ID 기반 모바일 학생증을 구현하였다. gRPC를 통해 서버와 통신하여 분산 ID 문서를 생성·발급하고, 사용자는 애플리케이션을 통해 검증 기관의 진위 판별 후 검증을 통해 블록체인에 발급 정보를 저장하게 되고 이후 서비스 이용이 가능하다. SSI로 개인정보 유출 위험성을 감소시킬 수 있고 특정 기관에 의존하지 않아 장기적으로 소유할 수 있다. 개인정보 공개를 최소화하며 필요한 정보를 선택적으로 제시할 수 있고, 모바일 플랫폼으로 서비스를 제공하여 플라스틱 카드를 소지하지 않아도 간편히 인증이 가능하여 편의성이 증가하는 장점이 있다.

본 논문이 제시한 모델은 누구나 열람이 가능한 블록체인 기반으로 구현했기 때문에 타 대학 간 교류에서도 필요할 때 활용이 가능하다. 또한, 대학교뿐만 아니라 기업과 기관에서도 사원증 및 교직원증과 같이 분산 ID를 활용하여 서비스를 확장할 수 있다. 또한, 특정 조직 내 정보체계와 연동하여 분산 ID로 발급된 인증서를 운용하는 등 분산 ID를 통해 더욱

안전하게 대학교 졸업증명서와 같이 필요한 정보를 오프라인과 온라인에서도 모든 개체에 대한 신뢰 높은 서비스 환경으로 이용할 수 있다.

최근 몇 년 사이에 대체 불가능 토큰 또는 ERC-721 토큰이라고도 불리는 NFT(Non-Fungible Token) 시장이 급성장하고 있다. NFT는 본래 이더리움의 토큰 표준에서 유래한 것으로, 각각의 토큰을 구별할 수 있는 기호로 구분하는 것을 목표로 하여 고유한 ID로 가상과 디지털 속성을 바인딩할 수 있다. NFT 기술이 가진 장점은 위조하기 어려운 복제 불가능한 희소성과 추적이 쉽도록 블록체인의 데이터를 공개적이고 투명하게 누구나 출처와 같은 정보들을 볼 수 있으며, 필요에 따라 개인의 신분을 보장할 수 있는 대체재로 사용할 수 있다는 것이다. 이러한 특징의 NFT를 신원증명에 사용하게 된다면, 신원정보를 복제하게 되더라도 기존의 NFT와는 다른 NFT를 덧붙이게 되므로 기존의 것과 구별될 것이다. 따라서 NFT 기술로 학생증을 이용하는 데 간편하면서도 신뢰 가능한 대체된 개인정보를 활용할 수 있도록 검토하여 향후 연구를 추진할 계획이다.

References

[1] Seung-Hyun Cho, Min-Jeong Kang, Ji-Yun Kang, Ji-Eun Lee, and Kyung-Hyune Rhee, "Development of Decentralized Identity-Based Mobile Student ID," CISC-S'21, pp. 383-386, Jun. 2021

[2] Jong-Gyu Park, Seong-Geun Kwon, Ki-Ryong Kwon, and Suk-Hwan Lee, "A Research on the Use of DID Using a Private Blockchain", 24(6), pp. 760-767, Jun. 2021

[3] W3C, "Decentralized Identifiers (DIDs)," https://www.w3.org/TR/did-core/#security-requirements, Aug. 2020

[4] Ki-Ho Yeo, Keun-Dug Park, and Heung-Youl Youm, "Proposal for a Custody and Federated Service Model for the Decentralized Identity," Journal of The Korea Institute of Information Security & Cryptology, 30(3), Jun. 2020

[5] COOV, "COOV," https://www.coov.kr, Aug. 2021

[6] PASS, "PASS," https://www.passauth.co.kr, Aug. 2021

[7] SK Telecom, "Initial," https://www.initial.id, Aug. 2021

[8] Coinplug, "MYKEEPiN," https://mykeepin.com, Aug. 2021

[9] BUSAN BLOCKCHAIN CITY, "B PASS," https://blockchainbusan.kr, Aug. 2021

[10] Blockchain Labs, "InfraBlockchain," https://infrablockchain.com/ko/technology, Aug. 2021

[11] SECUREKEY, "Verfied.Me," https://verified.me/how-it-works-what-is-verified-me, Aug. 2021

[12] ShoCard, "ShoCard ID Walle," https://www.shocard.com, Aug. 2021

[13] Y. S. Kim, Y.-S. Park, and B. Y. Lee, "Security Model of Smart Contract Based Private BlockChain Using Commitment Scheme," The Korea Contents Association, 18(7), pp. 620-627, Jul. 2018

[14] Kunews, "'KU Mobile ID', Using a student ID on smartphone," https://www.kunews.ac.kr/news/articleView.html?idxno=32453, Mar. 2021

[15] ThePublic, "Edubloc Platform launched a blockchain DID student card wallet called 'Eduwallet' for elementary and secondary school students," https://www.thepublic.kr/news/newsview.php?ncode=1065577495367778, Feb. 2021

〈저자소개〉

조 승 현 (Seung-Hyun Cho) 학생회원
2021년 8월: 부경대학교 IT융합응용공학과 학사
〈관심분야〉 보안공학, 모바일 보안, 리버스 엔지니어링, 모의해킹

강 민 정 (Min-Jeong Kang) 학생회원
2017년 3월~현재: 부경대학교 IT융합응용공학과 재학
〈관심분야〉 정보보호, IT융합

강 지 윤 (Ji-Yun Kang) 학생회원
2018년 3월~현재: 부경대학교 IT융합응용공학과 재학
〈관심분야〉 네트워크, 정보보호, IT융합

이 지 은 (Ji-Eun Lee) 학생회원
2018년 3월~현재: 부경대학교 IT융합응용공학과 재학
〈관심분야〉 정보보호, 프로그래밍, IT융합

이 경 현 (Kyung-Hyune Rhee) 종신회원
1982년 2월: 경북대학교 수학교육과 졸업
1985년 2월: 한국과학기술원 응용수학과 석사
1992년 8월: 한국과학기술원 수학과 박사
1985년 2월~1993년 2월: 한국전자통신연구원 연구원, 선임연구원
1993년 3월~현재: 부경대학교 IT융합응용공학과 교수
〈관심분야〉 정보보호, 암호이론, 암호 프로토콜, 통신보안, 블록체인 기반 기술 및 응용