Journal of the Korea Academia-Industrial cooperation Society
Vol. 21, No. 12 pp. 873-879, 2020

https://doi.org/10.5762/KAIS.2020.21.12.873
ISSN 1975-4701 / eISSN 2288-4688

블록체인 기반 안전한 마이데이터 서비스 모델

이광형[1], 정용훈[2*]
[1]서일대학교 소프트웨어공학과, [2]유니허브랩

Blockchain-based safety MyData Service Model

Kwang Hyoung Lee[1], Young Hoon Jung[2*]
[1]Department of Software Engineering, Seoil University
[2]UniHubLAB

요 약 4차 산업혁명의 핵심자원으로 데이터의 중요성이 부각되고 있으며, 기업에서는 개인 데이터를 불법적으로 수집하여 활용하고 있다. 금융권에서는 블록체인, 빅데이터, AI 기술 등을 활용하여 개인 데이터를 안전하게 관리하고 보다 좋은 서비스를 제공하기 위해 활발한 연구가 진행되고 있다. 본 논문에서는 블록체인 기술을 활용하여 개인 데이터를 안전하게 관리할 수 있으며, 기존 시스템 변동 없이 사용할 수 있는 시스템을 제안하였다. 본 시스템의 구성은 블록체인, 블록체인 연동, 서비스 제공기관, 사용자(App) 등으로 구성된다. 블록체인은 종류와 형태 상관없이 사용이 가능하며, 블록체인 연동 부분에서 블록체인 및 서비스를 구분하여 서비스를 제공한다. 서비스제공기관은 개인 데이터를 이용하기 위해 사용자에게 권한을 요청하고 위임 받아야만 개인 데이터에 접근이 가능하다. 기존 마이데이터 서비스는 사용자 휴대폰에 모든 데이터를 저장하므로 탈옥, 루팅으로 인해 정보가 유출될 수 있으나 제안하는 시스템에서는 블록체인에 개인 데이터를 저장하므로 정보 유출 사고를 방지할 수 있다. 추후 블록체인에 저장된 개인 데이터를 이용하여 맞춤형 서비스를 제공할 수 있도록 연구할 것이다.

Abstract The importance of data as a core resource of the 4th industrial revolution is emerging, and companies illegally collect and use personal data. In the financial sector, active research is conducted to safely manage personal data and provide better services using blockchain, big data, and AI technology. In this paper, we propose a system that can safely manage personal data by using blockchain technology, which can be used without changing the existing system. The composition of this system consists of a blockchain, blockchain linkages, a service provider, and a user (i.e., an app). Blockchain can be used regardless of its type and form, and services are provided by classifying blockchains and services in the blockchain linkages. Service providers can access personal data only after requesting and receiving delegated permission from users. Existent MyData services store all data in a user's mobile phone, so information may get leaked due to jailbreaks or rooting. But in the proposed system, personal data are stored in blockchain so information leakage can be prevented. In the future, we will study ways to provide customized services using personal data stored in blockchain.

Keywords : Blockchain, MyData, Authentication, Blockcahin Interlocking, Authority

본 논문은 2020년도 서일대학교 학술연구비에 의해 연구되었음.
*Corresponding Author : Yong-Hoon Jung(UniHubLAB)
email: jung7773@naver.com
Received October 16, 2020 Revised November 11, 2020
Accepted December 4, 2020 Published December 31, 2020

1. 서론

4차 산업혁명의 핵심자원으로는 데이터의 중요성이 부각되는 가운데 정보주체인 개인이 소외되는 정보보호 문제와 빈번한 유출사고 문제가 대두 되고 있다. 개인이 자기정보를 관리, 통제하기 어려워지면서, 소극적인 정보보호만으로는 개인정보 자기결정권의 보장에 한계가 있다. 데이터 활용에 대한 논의도 기업을 중심으로 이루어지고 있으며, 데이터 기반의 혁신의 혜택에서 정보주체가 배제될 우려도 제기되고 있다.

마이데이터는 정보주체인 개인의 데이터 활용도를 높이고 우수한 역량을 가진 업체가 대형 금융기관과 대등하게 경쟁할 수 있는 환경을 조성할 것으로 기대를 모으고 있다.

마이데이터 서비스는 의료 및 헬스케어 산업 분야에서 활발하게 연구되고 있다. 기존 의료 및 헬스케어 산업 분야에서는 의료 정보 및 건강에 관련된 정보를 수집하여 의료 목적에 사용하고 있다. 하지만 의료기관 상호간에 의료정보가 공유되지 않으므로 개인은 의료기관 이동 시마다 같은 검사를 중복해야 하는 불편함이 있다. 정부에서는 이러한 문제를 해결하기 위해 의료정보공유시스템 개발을 위해 노력하였으나 의료 업계 반대로 성공할 수 없었다.

현재 마이데이터 서비스는 개인의 데이터를 대부분 휴대폰에 저장하고 있다. 하지만 휴대폰은 탈옥(jailbreak), 루팅(looting)으로 인해 해킹 사고가 발생할 수 있으므로 안전하지 않다.

제안하는 시스템에서는 개인의 다양한 데이터를 스마트폰이 아닌 블록체인에 비식별화하고 분산 저장하여 안전하게 관리할 수 있다. 3장에서는 기존 서비스를 그대로 이용할 수 있으며, 보다 안전한 마이데이터 서비스를 제안한다. 4장에서는 기존 시스템과의 성능 비교는 무의미하여 기존 시스템과 안전성, 편의성, 확장성을 비교 분석하였다.

2. 관련연구

2.1 금융권

현재 정보 주체인 개인의 금융데이터 활용도는 그다지 높지 않다. 특히 본인 데이터를 활용하여 자산을 통합적으로 관리하기가 불편한 상황이다. 개인이 직접 통합 자산관리를 수행하기에는 본인에 대한 데이터가 여러 금융기관에 분산되어 보관되고 있기 때문에 이를 체계적으로 수집하거나 활용하기가 어렵다. 개별 금융기관은 고객들의 거래 및 지출, 투자내역을 각자 축적하고 이를 분석하여 자체적인 마케팅에 활용하지만, 고객들의 타 금융기관 이용내역을 확인할 수 없어 고객 중심의 통합 자산관리 서비스를 제공하는 데에는 한계를 지닌다.

금융권에서 마이데이터는 계좌통합조회 서비스를 꼽을 수 있다. 이는 고객의 동의하에 여러 금융기관에 개설된 계좌의 잔액과 거래 내역 등 개인금융정보를 하나의 화면에 모아 표시해주는 서비스를 말한다. 또한 고객을 대신하여 가계부를 자동으로 작성하고 소비패턴을 분석하고 이에 따른 맞춤형 금융상품을 추천하는 등 개인금융데이터를 활용하여 다양한 부가서비스를 제공하고 있다. 개인금융데이터를 수집하는 방식은 크게 두 가지다.

첫째는 스크린 스크레핑(screen scraping)으로 고객에게 입력 받은 개별 금융기관의 아이디와 비밀번호 또는 공인인증서를 통해 업체가 금융기관의 웹사이트에 대리 접속하고 고객 데이터를 수집하는 방식이다. 금융기관의 명시적 허가 없이도 업체가 고객을 대신하여 데이터를 수집할 수 있어 현재 활발하게 쓰이고 있다. 그러나 데이터 수집 속도가 느리고, 고객의 계정 정보가 탈취당할 위험이 존재하며, 업체가 서비스 내용 외 고객의 다른 개인정보에 접근할 수 있다는 문제가 존재한다.

둘째는 응용프로그램 인터페이스(Application Programming Interface : API)로, 웹사이트가 아닌 별도의 프로그래밍 전용 인터페이스를 통해 금융기관이 업체에게 데이터를 전송하는 방식이다. API는 데이터 전송에 특화되어 있기 때문에 스크린 스크레핑에 비해 훨씬 빠르고 안전하며 효율적이다. 고객의 계정 정보가 노출될 우려가 작고, 고객이 동의하지 않은 데이터 영역에는 업체의 접근이 불가능하며, 데이터 업데이트 여부를 실시간으로 알려줄 수도 있다. API는 기능면에서 이토록 우월하지만 현재 국내 계좌통합조회 서비스에서 실제 활용되는 빈도는 그리 많지 않다. API 활용을 위해서는 개별 금융기관이 스스로 이를 개발하고 외부에 공개해야만 하는데 그렇게 할 만한 유인이 아직까지 크지 않기 때문이다[6][8].

2.2 비금융권

의료 분야에서는 건강검진 및 처방전 데이터를 개인이 휴대폰 앱에서 직접 내려받아 제3의 기업에게 제공하여 맞춤형 건강관리(활동량, 영양관리 등) 및 식단추천 서비스에 활용할 수 있도록 한다. 이에 따라 기존에 서면, CD

등 활용이 어려운 형태로 제공되던 개인 건강검진 결과 및 처방내역을 휴대폰 앱으로 손쉽게 관리·활용할 수 있으며, 본인의 건강 상황에 맞는 식단을 제공하고 주문·결제를 연계하여 개인의 편리한 건강관리를 돕는다.

에너지 분야에서는 가구별 에너지(상·하수도, 전력, 가스 등) 사용량 데이터를 활용하여 시간대별 사용량 모니터링 및 시각화 분석, 누진제 적용 시작 구간 알람 등의 에너지 절감 서비스를 제공한다. 이에 따라 기존에는 월 단위로 확인할 수밖에 없었던 사용량을 시간대별로 확인하여 가구 스스로 사용량을 관리할 수 있게 되며, 유사가구 등과의 사용량 비교분석을 통해 이상징후(이상 가스 패턴, 누수, 누진 등)를 조기 파악하는 등 가계 에너지 요금 절감에 기여할 수 있게 된다[9].

2.3 블록체인

블록체인은 공공 거래 장부로 불리는 데이터 분산 처리기술을 의미한다. 블록체인은 네트워크에 참여하는 모든 사용자가 모든 거래 내역 등의 데이터를 분산, 저장하는 기술을 말한다.

블록체인에서 블록은 개인과 개인의 거래(P2P)의 데이터가 기록되는 장부를 말한다. 이런 블록들은 형성된 후 시간의 흐름에 따라 순차적으로 연결된 체인 구조를 가지게 된다.

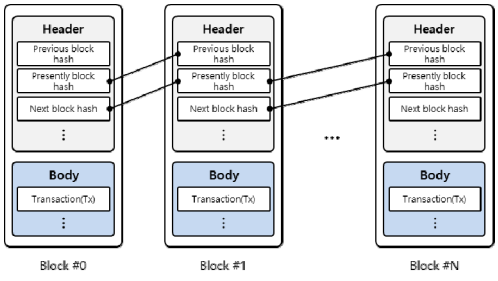

Fig. 1. Blockchain Structure

모든 사용자가 거래 내역을 보유하고 있어 거래 내역을 확인할 때는 모든 사용자가 보유한 장부를 대조하고 확인해야 한다.

기존 거래 방식에서는 중앙 서버를 공격하는 방식으로 데이터 위변조가 가능했다. 블록체인은 데이터를 여러 명이 나누어 저장하기 때문에 위변조가 어렵다는 특징을 가진다. 블록체인 네트워크를 위변조하기 위해서는 참여자의 거래 데이터를 모두 공격해야하기 때문에 사실상 해킹은 불가능하다.

또한 블록체인은 다수가 데이터를 저장, 증명하기 때문에 중앙 관리자가 존재하지 않는다[9].

최근 블록체인 환경에서 사용자 인증, 사용자 식별 등에 대한 연구가 활발하게 진행되고 있다. 여러 민간 기업들은 DID 얼라이언스를 출범하고 분산ID(DID) 제품을 출시하고 있으며, 대학 및 연구소에서는 논문을 통해 발표되고 있다[1-5][7][10].

3. 본론

본 논문에서 제안하는 마이데이터(MyData) 서비스는 블록체인에 개인 데이터를 분산 저장하여 안전하게 관리할 수 있는 서비스를 제안한다.

제안하는 시스템에서는 제공기관의 형태에 따라 별도의 블록체인을 구성할 수 있으며, 블록체인 종류에 제한 없이 사용 가능하다. 제안하는 시스템에서는 사용자(App), 서비스 제공기관, 블록체인 연동, 블록체인으로 구성된다. 다음은 전체 시스템 구성이다.

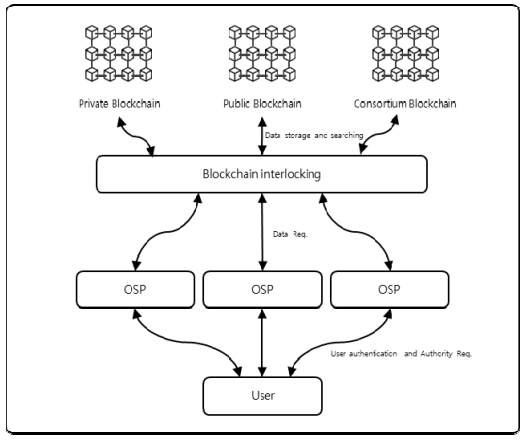

Fig. 2. system configuration

블록체인에 저장된 정보는 블록체인 연동을 통해서만 접근이 가능하며, 사용자는 본인확인 후 자신의 정보에만 접근이 가능하다. 서비스 제공기관은 사용자에게 접근하고자 하는 정보에 대한 접근 권한을 획득해야만 접근이 가능하다.

3.1 제안하는 시스템

블록체인은 서비스 형태에 따라 별도로 구성할 수 있으며, 금융 또는 본인확인 기관 등은 Private Blockchain

으로 구성한다. 일반적인 증명서를 서비스하는 경우 Public Blockchain 또는 Consortium Blockchain으로 구성할 것을 권장한다.

3.1.1 블록체인

블록체인은 Public, Private, Consortium Blockchain 모두 구성이 가능하며, 블록체인의 종류(비트코인, 이더리움, 이오스 등)는 제한이 없다. 단 블록체인은 서비스 제공기관 또는 정보의 종류에 따라 선택적으로 구축할 수 있다.

제안하는 시스템은 개인 데이터를 저장하기 위해 속도가 빠른 이오스(EOS)를 기반으로 Public Blockchain을 구성하였다.

3.1.2 블록체인 연동(Interlocking Center : IC)

블록체인 연동에서는 다양한 블록체인의 종류를 모두 사용할 수 있도록 블록체인을 구분하는 역할을 한다. 블록체인 연동 부분은 서비스 형태에 따라 App 내에도 설치가 가능하다.

블록체인 연동에서는 서비스 제공기관이 개인 데이터에 접근 시 권한을 확인하고, 권한이 있는 경우에만 데이터 접근을 허가 한다.

서비스 제공기관에서 마이데이터 서비스를 하는 경우 시스템 연동을 위해서는 블록체인 연동에 프로그램을 설치함으로서 사용자에게 서비스를 제공할 수 있다. 서비스 제공기관에서 제공되는 서비스의 종류와 상관없이 이용 가능하다.

3.1.3 서비스 제공기관(OSP)

서비스 제공기관에서는 사용자의 개인 데이터에 접근하기 위해서는 권한을 부여 받아야 접근이 가능하다. 또한 사용자 본인인증은 필수로 하며, 본인인증에는 ID/PW, 공인인증서, DID 등 모두 사용 가능하다. 본 논문에서는 DID를 기준으로 권한을 요청하고 권한을 위임하는 방법을 사용한다.

가) 권한 요청

개인 데이터에 접근하기 위해서는 사용자에게 권한을 요청해야 하며, 권한 요청 메시지는 다음과 같이 생성한다.

$$Request\,Message = OSP\,DS \| OSP\,DID \| User\,DID \| User\,Datatype \| Blockchain\,Code \quad (1)$$

OSP DS is the digital signature of service provider, OSP DID and User DID are service provider and user DID, User Datatype is user data type, Blockchain code is blockchain type

$$OSP\,DS = E_{OSP\_Pri\_Key}(OSP\,DID \| User\,Datatype \| Blockchain\,Code) \quad (2)$$

OSP DS is a digital signature method for service providers. $E_{OSP\_Pri\_Key}$ is the private key of the service provider.

Eq. (1)은 권한 요청 메시지의 전체이다. OSP DS는 서비스 제공기관의 전자서명이며, OSP DID는 서비스 제공기관의 분산아이디(DID)이다. User Datatype은 사용자의 데이터 종류를 의미한다.

Eq. (2)는 전자서명 생성 방법이다. 서비스 제공기관 전자서명에는 사용자의 데이터 종류와 데이터가 저장된 블록체인 코드를 요청한다. 이를 통해 권한 요청 메시지가 서비스 제공기관이 보낸 것이 맞는지를 확인한다.

사용자는 권한 요청 메시지를 수신하고 이에 대한 응답으로 서비스 제공기관에 권한을 위임할 수 있다.

3.1.4 사용자(App)

사용자는 개인 데이터를 App을 통해 블록체인에 저장 및 사용할 수 있으며, 서비스 제공기관에서 개인 데이터 접근 권한 요청 시 권한을 부여하여 접근할 수 있도록 한다.

제안하는 시스템 이용 시 App은 필수로 설치해야 하며, App 접근 시 본인인증은 필수이다.

가) 권한 위임

서비스 제공기관으로부터 권한 요청 메시지를 수신한 경우 서비스 제공기관에 대한 인증 후 요청 메시지에 대한 응답 메시지를 작성하여 응답한다. 권한 요청 메시지에 대한 응답 메시지는 다음과 같이 생성한다.

$$Response\,Message = User\,DID \| User\,DS \| OSP\,DID \| Authority \quad (3)$$

This is the entire response message. Authority is the allow and deny values.

$$User\,DS = E_{User\_Pri\_Key}(User\,DID \| OSP\,DID) \quad (4)$$

This is the user's digital signature value.

$$Authority = E_{User\_Pri\_Key}(Blockchain\ Code \| Data\ Type \| Accept \text{ or } Denial) \quad (5)$$

Authority is the result of authority. Blockchain codes, data types, and authority values are encrypted with the user's private key.

Eq. (3)은 권한 요청에 대한 응답 메시지 전체를 나타낸다. Eq. (4)는 사용자의 전자서명 값이다. Eq. (5)는 사용자가 서비스 제공기관에게 권한을 부여하는 식으로 정보가 저장된 블록체인 코드와 데이터 종류 그리고 권한 부여 및 거부값을 사용자의 개인키로 암호화된다.

사용자는 권한을 위임함으로서 다양한 서비스와 정보 제공에 대한 대가를 제공받을 수 있다.

다음은 권한 위임 요청 및 획득하는 전체 데이터 흐름을 나타낸다.

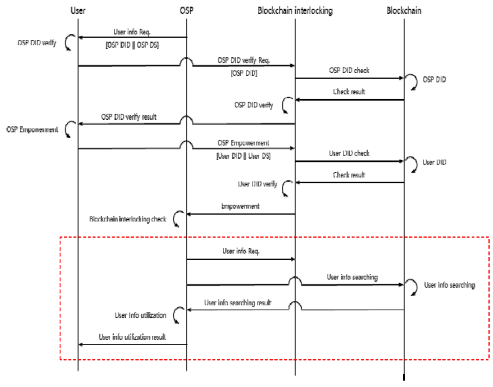

Fig. 3. Request for permission

서비스 제공기관에서 사용자에게 권한 요청과 권한 위임을 받기 위한 순서는 다음과 같다.

① 서비스 제공기관(OSP)는 사용자 정보를 이용하기 위해 권한 요청

② 사용자는 OSP의 전자서명을 확인한 후 DID를 Blockchain interlocking(IC)에게 검증 요청

③ Blockchain interlocking에서는 블록체인에 저장된 OSP DID를 조회하여 검증한 후 검증 결과를 사용자에게 전송

④ 사용자는 검증 결과에 따라 Blockchain interlocking에게 OSP에게 권한을 위임 또는 거부

⑤ Blockchain interlocking에서는 사용자의 전자서명 확인 후 블록체인에 저장된 DID를 조회하여 검증

⑥ 사용자 DID 검증 후 Blockchain interlocking에서는 OSP에게 권한 위임 및 거부 사실 전송

⑦ OSP는 Blockchain interlocking 또는 직접 블록체인에서 사용자 정보에 접근 및 이용

⑧ 사용자에게 정보 이용 결과 전송

4. 실험평가

성능분석은 안전성을 중심으로 하였으며, 편의성과 확장성을 추가로 고려하였다. 안전성은 다양한 공격 방식과 보안 침해 요소, 편의성 및 확장성은 데이터 저장 방법 및 권한 위임, 확장성 등으로 한다.

4.1 안전성

기존 마이테이터 서비스는 사용자의 휴대폰에 개인 데이터를 저장함으로써 휴대폰 탈옥, 루팅을 통한 해킹 사고에 노출되어 있다.

제안하는 시스템은 개인 데이터를 휴대폰에 저장하지 않고 블록체인에 분산 저장하여 안전하게 관리할 수 있다. 또한 개인 데이터에 접근하기 위해서는 권한을 위임받아야 하며, 권한을 획득하기 위해서는 개인정보가 유출되지 않는 분산 ID를 사용하였다.

제안하는 마이데이터 서비스는 블록체인에 개인 데이터를 저장하므로 악의적인 위·변조를 방지할 수 있다. 블록체인에 저장된 블록은 변경할 수 없으므로 등록된 데이터는 수정 및 삭제가 불가능하다.

Table 1. Safety comparison

	Nomal	MyData	Proposal
Storage location	Server	phone	blockchain
Authentication method	ID/PW	ID/PW, FIDO	ID/PW, Certification FIDO DID
rooting/ Jailbreak	-	O	X
safety	X	X	O
network	client-Server	phone-server	phone-blockchain
Integrity	X	△	O
immutability	X	△	O
Transparency	X	O	O

성능 평가를 위해 Server-Client 시스템, 기존 MyData 서비스, 제안하는 시스템으로 비교하였다. 비교는 저장위치, 인증 방법, 해킹(탈옥, 루팅) 가능 여부, 안전성 등을 비교하였다.

기존 서비스 제공기관에서는 정보를 서버에 저장하였으며, MyData 서비스는 사용자의 스마트폰에 정보를 저장하여 해킹사고가 발생하였다. 제안하는 시스템은 정보를 블록체인에 분산 저장하므로 하나의 서버 또는 스마트폰이 아닌 블록체인에 분산되어 있으므로 안전하다.

Server-Client 방식은 ID/PW, 공인인증서 등 소유기반 중심의 사용자 인증을 하였다. 기존 MyData 서비스는 ID/PW 또는 생체인식(FIDO)을 혼용하여 사용하고 있다. 제안하는 시스템에서는 ID/PW, 인증서, 생체인식, DID 등 다양한 인증 방식을 사용할 수 있다.

해킹에 대한 안전성은 스마트폰 기반의 MyData와 제안하는 시스템을 비교한다. 스마트폰(android, iOS)은 루팅과 탈옥으로 인해 사고가 빈번하게 발생할 수 있으며, 정보가 스마트폰에 저장되므로 안전하지 않다. 제안하는 시스템은 블록체인에 정보가 저장되므로 루팅이나 탈옥을 통해 획득할 수 있는 정보가 없으므로 안전하다.

데이터에 대한 무결성, 불변성, 투명성에 대해서는 블록체인에 저장된 정보를 수정하기 위해서는 51% 이상의 정보를 동시에 수정해야 하므로 거희 불가능하다. 그러므로 데이터의 무결성, 불변성, 투명성 또한 보장된다.

블록체인에 저장된 데이터는 읽기 권한이 있는 노드들은 네트워크에 배포되거나 등록된 트랜잭션을 실시간으로 열람할 수 있다. 블록체인에 등록된 데이터는 계정(DID)를 기반으로 사용자, 서비스이용기관 등 이용 및 요청 기록을 확인할 수 있으므로 불법적인 행위 추적이 가능하다.

4.2 편의성 및 확장성

4.2.1 편의성

기존 마이데이터 서비스는 서비스 제공기관에 따라 다양한 형태의 데이터 포맷을 사용해야 하며, 이에 따른 전용 프로그램이 필요하다. 제안하는 마이데이터 서비스는 하나의 앱을 통해 서비스제공기관의 프로그램 종류와 상관없이 사용이 가능하다.

서로 다른 서비스제공기관이 제공하는 서비스 이용을 위해 블록체인 연동 부분에서는 서비스를 구분하여 지원한다.

4.2.2 확장성

제안하는 마이데이터 서비스는 기존 어떤 서비스와도 변동 없이 사용이 가능하도록 설계하였다. 기존 서비스를 사용하기 위해서는 블록체인 연동 부분에 서비스를 위한 프로그램을 설치하면 사용이 가능하다. 블록체인 연동 부분에서는 블록체인, 클라우드, 데이터베이스 등 서비스 연동이 가능하며, 기존 클라우드와 데이터베이스에 저장된 정보를 블록체인에 저장할 수도 있다.

5. 결론

최근 다양한 분야에서 마이데이터 서비스에 대한 연구가 활발하게 진행되고 있다. 현재까지 마이데이터 서비스는 사용자의 휴대폰에 개인 데이터를 저장하는 형태로 탈옥이나 루팅으로 인해 개인 데이터의 유출로 이어질 수 있다.

제안하는 시스템에서는 개인 데이터를 안전하게 보관할 수 있도록 블록체인에 개인 데이터를 저장하는 서비스를 제안하였다. 블록체인에 저장된 정보를 해킹하기 위해서는 51% 이상의 정보를 동시에 해킹해야만 가능하므로 개인 데이터의 무결성, 불변성, 투명성 등을 보장할 수 있다.

개인 데이터를 서비스 제공기관이 불법적으로 사용하는 것을 방지하기 위해 사용자와 서비스 제공기관에게 DID와 생체인증 기반 인증을 통해서만 정보를 제공할 수 있도록 하였다. 또한 개인 데이터에 접근하기 위해서는 권한 요청을 통해 권한을 위임 받아야만 접근이 가능하다.

현재 개인데이터를 저장하기 위해 휴대폰과 클라우드, 데이터베이스를 사용하고 있으나 해킹에 대한 위험성이 존재하므로 블록체인을 사용하였다. 블록체인은 종류에 상관없이 사용이 가능하며, 기존 사용자 휴대폰, 클라우드, 데이터베이스 사용자도 이용이 가능하도록 설계하였다.

향후 빅데이터, AI를 연계하여 개인 데이터 활용에 대한 방안과 서비스 도출 방안, 개인 데이터 활용 대가를 자동 산정할 수 있도록 개선할 것이다.

References

[1] Kim Jai-Yong, Jung Yong-hoon, Jun Moon-Suk, Lee Sang-Beon, “User Integrated Authentication System

using EID in Blockchain Environment", Journal of the Korea Academia-Industrial cooperation Society, Vol.21, No.3, pp.24-31, Mar. 2020.
DOI : http://dx.doi.org/10.5762/KAIS.2020.21.3.24

[2] Song Mi-Jeong, "A Study on Reinforcement of Personal Information Protection of My Data Policy in the Domestic Financial Field", Master degree, Korea University, 2020.

[3] Kwon Min-Kyung, "Current status and implications of domestic and overseas my data introduction", Korea Capital Market Institute, Korea, 2019.

[4] Korea Data Agency, "2019 Data Industry White Paper", 2019 Data Industry White Paper, Korea, Vol.22, 2018.

[5] S. D. Yoo, "A Study on Consensus Algorithm based on Blockchain", The Journal of The Institute of Internet, Broadcasting and Communication , Vol.19, No.3, pp.25-32, 2019.
DOI : https://doi.org/10.7236/JIIBC.2019.19.3.25

[6] S. J. Han, S. T. Kim, S. Y. park, "A GDPR based Approach to Enhancing Blockchain Privacy", The Journal of The Institute of Internet, Broadcasting and Communication , Vol.19, No.5, pp.33-38, 2019.
DOI : https://doi.org/10.7236/JIIBC.2019.19.5.33

[7] S. G. Moon, M. S. Kim, H. J. Kim, "Design of an Integrated University Information Service Model Based on Block Chain", Journal of the Korea Academia-Industrial cooperation Society Vol. 20, No.2 pp. 43-50, 2019.
DOI : https://doi.org/10.5762/KAIS.2019.20.2.43

[8] Financial Services Commission, "A plan to introduce my data industry in the financial field for consumer-oriented financial innovation", Detailed implementation plan for the comprehensive plan for data utilization and information protection in the financial sector, Korea, 2018.

[9] National Information Society Agency, "The rise of the data economy and its socioeconomic impact", IT&Future Strategy, Korea, 2018.

[10] W3C Working Draft "Decentralized Identifiers (DIDs) v1.0", 14 July 2020, https://www.w3.org/TR/did-core (accessed Aug. 7, 2020)

이 광 형(Kwang-Hyoung Lee) [종신회원]

- 1998년 2월 : 광주대학교 컴퓨터공학과 졸업(공학사)
- 2002년 2월 : 숭실대학교 컴퓨터공학과 (공학석사)
- 2005년 2원 : 숭실대학교 컴퓨터공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학 소프트웨어공학과 부교수

〈관심분야〉
멀티미디어 데이터 검색, 영상처리, 멀티미디어 보안, 학습콘텐츠, AI

정 용 훈(Yong-Hoon Jung) [종신회원]

- 2006년 8월 : 숭실대학교 일반대학원 컴퓨터학과(공학석사)
- 2010년 2월 : 숭실대학교 일반대학원 컴퓨터학과(공학박사)
- 2011년 3월 ~ 2014년 2월 : 서일대학교 조교수
- 2018년 8월 ~ 현재 : 바스랩 연구소장
- 2019년 11월 ~ 현재 : 유니허브랩 기술이사 겸직
현) 한국산학기술학회 상임이사

〈관심분야〉
블록체인, 사용자 인증, 네트워크 보안, 융합 보안