Journal of the Korea Academia-Industrial cooperation Society
Vol. 23, No. 11 pp. 865-871, 2022

https://doi.org/10.5762/KAIS.2022.23.11.865
ISSN 1975-4701 / eISSN 2288-4688

블록체인 기반 IoT 센서와 RFID Active Tag를 이용한 객체 추적

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

Object tracking using blockchain-based IoT sensor and RFID Active Tag

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

요 약 최근 코로나로 인해 개인 모빌리티 산업이 발전하고 있으며, 다양한 모빌리티 서비스를 사용하고 있다. 개인 모빌리티 서비스는 회원제로 운영되고 있으며 회원가입 후 사용이 가능하도록 되어 있다. 하지만 본인확인 절차가 미흡하여 타인 명의로 서비스 이용이 가능하며, 이로 인한 문제점이 대두되고 있다. 본 논문에서는 블록체인 기술을 이용해 객체를 추적할 수 있는 서비스를 제공한다. 사용자 EID 발급 시 본인명으로 개설된 스마트폰을 기본으로 하여 타인에게 양도가 불가능하도록 하였으며, 객체 EID는 제조사와 객체 고유 일련번호를 사용하였다. 또한 객체를 추적하기 위해 서비스 이용 시 본인확인에 사용된 사용자 EID와 객체 EID를 매칭하였으며, IoT 센서와 Active Tag 위치정보를 활용하여 서비스 이용에 대한 부인방지와 정확한 위치정보를 전송할 수 있도록 하였다. 실험 평가는 사용자 EID와 객체 EID에 대한 안전성, 무결성, 위변조 등을 기존 시스템과 비교하였다. 제안하는 시스템에서는 블록체인 기술을 이용하여 사용자 EID와 객체 EID 발급하고 이를 기반으로 서비스 시작부터 서비스 종료까지 모든 구간을 추적할 수 있도록 하였다. 서비스 이용 시 스마트폰에 저장된 사용자 EID는 타인에게 양도가 불가능하므로 보다 정확한 본인확인과 부인방지 서비스를 제공할 수 있다.

Abstract Recently, the personal mobility industry has been developing more rapidly due to the novel coronavirus, and various mobility services are used. Personal mobility services operate on a membership system and can only be used after registration. However, owing to insufficient identity verification processes, it is possible to use a service by using the name of another person, and problems are emerging. In this paper, we provide a service that can track objects using blockchain technology. When issuing a user's EID, it is impossible to transfer it to another person because the smartphone is associated with the original person's name. For the object's EID, the serial numbers of the manufacturer and the device are used. In addition, in order to track the object, both the user EID and the object EID are used for identification when using the service and they must match. IoT sensor and Active Tag location information are used to prevent non-repudiation of service use and to transmit accurate location information. Experimental evaluation compared the safety, integrity, and forgery risk of the user EID and object EID associated with the proposed system. In it, user EID and object EID are issued using blockchain, and based on this, all accesses from service start to service end can be traced. When using the service, the user EID stored in the smartphone cannot be transferred to another person, so more accurate identification and a non-repudiation service can be provided.

Keywords : Blockchain, EID, Active Tag, Authentication, IoT

본 논문은 2022년도 서일대학교 학술연구비에 의해 연구되었음.
*Corresponding Author : Young-Hoon Jung(UniHubLAB)
email: jung7773@naver.com
Received October 4, 2022 Revised November 2, 2022
Accepted November 4, 2022 Published November 30, 2022

1. 서론

최근 신종 코로나바이러스 감염증이 확산되면서 서울과 경기도 등 수도권을 중심으로 대중교통을 꺼리는 사람들이 많이 생겨나고 있다. 대중교통은 불특정 다수와의 접촉이 발생하는 공간이므로 누구나 바이러스에 노출될 수 있다.

그로 인해 개인화 서비스에 큰 관심이 모아지고 있으며, 1인 모빌리티 공유 서비스에 관심이 집중되고 있다. 모빌리티 공유 서비스는 일반적으로 사람들의 이동을 편리하게 하는데 기여하는 각종 서비스나 이동수단을 폭넓게 일컫는 말로 사용되고 있다.

코로나 바이러스로 인해 개인 모빌리티 산업이 발전하면서 전동식 퀵보드, 공유 자전거, 카쉐어링 등 다양한 개인 모빌리티 서비스가 발달하고 있다. 가까운 거리를 이동하거나 교통 혼잡이 있을 경우 쉽고 빠르게 이용할 수 있는 전동 퀵보드 또는 공유 자전거를 이용하는 사용자가 급증하고 있다.

또한 장거리 이동 시 기차, 고속버스, 비행기 등을 이용하고 이동한 지역에서는 카쉐어링 서비스를 이용하는 경우가 많이 생겨나고 있다.

모빌리티 서비스는 개인이 소유하지 않고 공유함으로써 금전적인 부담을 줄여주고, 편리함을 제공한다.

하지만 모빌리티 서비스 이용 시 개인에 대한 본인확인에 대해서는 미흡한 상태이다. 최근 모빌리티 서비스 등장으로 다양한 사고가 발생하고 있으며, 사고 발생 시 책임소재에 대한 문제점과 전동식 퀵보드, 공유 자전거, 카쉐어링 등을 추적할 수 있는 시스템은 CCTV에 의존하고 있다.

제안하는 논문에서는 블록체인 기술과 IoT 센서, RFID Tag를 이용하여 모빌리티 서비스 이용자의 본인확인 방법과 모빌리티 객체를 추적할 수 있는 시스템을 제안한다. 제안하는 시스템에서 사용하는 본인확인 기술은 학생증, 사원증, 의료보험증 등으로 활용이 가능하며, 향후 전동식 퀵보드, 자전거, 자동차 생산 업체에서 제품 생산 시 RFID Tag를 부착하여 제작한다면 저렴한 비용으로 개발이 가능하다.

3장에서는 제안하는 시스템에 대한 각각의 역할, 기능, EID 발급 방법 등을 기술한다. 4장에서는 제안하는 시스템 안전성과 편의성, 확장성을 기준으로 기존 시스템과 비교 분석을 통해 우수성을 입증하였다.

2. 관련 연구

2.1 블록체인

블록체인은 공공 거래 장부로 불리는 데이터 분산 처리기술을 의미한다. 블록체인 네트워크에 참여하는 모든 사용자가 거래 내역 등의 데이터를 분산, 저장하는 기술을 말한다. 블록체인에서 블록은 개인과 개인의 거래(P2P) 데이터가 기록되는 장부를 말한다. 이런 블록들은 형성된 후 시간의 흐름에 따라 순차적으로 연결된 체인 구조를 가지게 된다[1].

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 가능하다. 블록체인 기술은 데이터를 여러 명이 나누어 저장하기 때문에 위변조가 어렵다는 특징을 가진다. 블록체인 네트워크를 위변조하기 위해서는 참여자의 거래 데이터를 모두 공격해야 하기 때문에 사실상 해킹은 불가능하다. 또한 블록체인은 다수가 데이터를 저장, 증명하기 때문에 중앙 관리자가 존재하지 않는다[2,3].

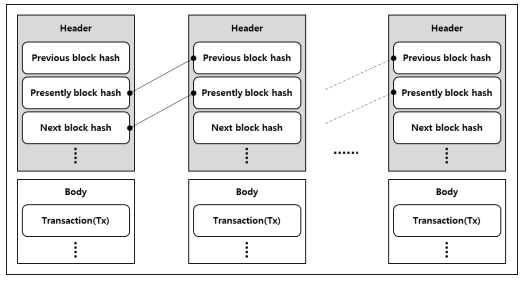

Fig. 1. Blockchain Structure

최근 블록체인 환경에서 사용자 인증, 사용자 식별 등에 관한 연구가 활발하게 진행되고 있다. 현재 W3C Working Group에서는 DID draft v1.0을 공개하고 있다. 국내에서도 DID를 이용한 모바일 신분증 사업이 진행되어 사용되고 있다[4-6].

2.2 사용자 인증

사용자 인증 방법으로는 ID/PW, 공인인증서, 생체인증, 간편인증 등 다양한 방법을 사용하고 있다.

2.2.1 간편인증

간편인증이란 PIN 번호, 바이오 정보, 패턴 입력 등 간편한 방법으로 본인확인 및 전자서명 서비스를 이용하는 방식이다. 간편인증 서비스 중 카카오, 네이버, 통신사 등이 제공하는 서비스가 가장 많이 사용되고 있다[7-9].

2.2.2 PKI(Public Key Infrastructure)

과거 인터넷이나 인트라넷 상의 사용자들에게 보안 서비스를 제공하는 체계로 공개키 기반구조(PKI), 국가 공개키 기반구조(NPKI, National Public Key Infrastructure)가 사용되었다. 현재 공개키 기반구조는 그대로 사용되고 있으나 공인인증서가 아닌 공동인증서, 금융인증서 등으로 발급 주체가 변경되고 이름이 변경되어 사용되고 있다.

사용자는 인증기관, 은행, 증권사를 통해 공동인증서를 발급 및 재발급하여 사용할 수 있다.

공동인증서는 인터넷상에서 전자거래 등을 안심하게 사용할 수 있도록 해주는 사이버 증명서로 전자서명을 하면 상대방이 서명한 사람이 누구인지를 확인할 수 있으며, 전자문서의 위변조 예방 및 거래 사실을 증명할 수 있다[1-3].

2.2.3 DID(Decentralized Identifier)

W3C Working group 에서는 분산 신원확인 기술에 대해 표준화를 추진하고 있다. W3C 분산 신원확인 기술은 검증 가능하고 탈중앙화된 디지털 신원을 증명하기 위한 새로운 형식의 식별자를 말한다. 이러한 새로운 식별자는 DID 컨트롤러가 DID의 제어권을 증명하고, 중앙화된 레지스트리, 신원 제공자, 인증기관 등으로부터 독립적으로 구현할 수 있도록 설계하고 있다.

DID는 DID 주체와 관련된 URL로써, DID 문서라는 방식을 통해 해당 주체와 신뢰할 수 있는 상호작용을 가능케 하는 도구이다. DID문서는 특정 DID를 어떻게 사용하는지에 대한 간단한 설명 문서이다. 각 DID 문서는 암호학적 요소, 검증 메소드 서비스 엔드포인트 등으로 표현될 수 있다. 해당 요소들은 DID 컨트롤러가 DID의 통제권에 대한 증명을 가능하게 하는 메커니즘 집합을 제공한다. 서비스 엔드포인트는 DID주체와 신뢰할 수 있는 상호작용을 가능하게 한다[10].

3. 본론

본 논문에서는 블록체인 기술을 이용하여 사용자와 객체에 EID를 발급하고 RFID와 IoT 센서를 이용하여 객체를 추적할 수 있는 시스템을 제안한다.

본인확인을 위한 사용자 EID(Electronic IDentification) 발급 시 본인명으로 발급된 스마트폰을 기본으로 하여 타인에게 양도가 불가능하도록 하였다.

객체 EID는 제조사와 객체에 고유 일련번호를 사용하여 발급한다. 또한 객체 추적을 위해 서비스 이용 시 본인확인에 사용된 사용자 EID와 객체 EID를 매칭하였으며, IoT 센서와 Active Tag 위치정보를 활용하여 서비스 이용에 대한 부인방지와 정확한 위치정보를 전송할 수 있도록 하였다.

객체에 내장된 Active Tag는 주기적으로 IoT 센서에 신호를 보내며, IoT 센서의 위치와 객체에 내장된 Active Tag의 위치 정보를 조합하여 객체를 추적할 수 있다. 다음 Fig. 2는 제안하는 시스템에 대한 구성이다.

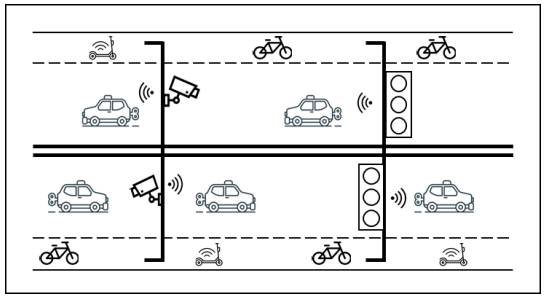

Fig. 2. Proposed system

사용자 EID는 블록체인과 스마트폰에 저장되며 객체 EID 발급은 관리기관을 통해 발급되며, 발급된 객체 EID는 블록체인에 저장된다.

3.1 사용자 EID 발급

사용자 EID 발급에는 사용자 스마트폰이 있어야 하며 사용자 이름, 전화번호와 스마트폰 IMEI 값이 사용된다. 사용자 EID 발급 절차는 Fig. 3과 같으며 다음과 같은 절차에 따라 진행된다.

사용자 EID 발급 절차

① EID 발급 요청(User name || Phone No. || IMEI)

② 사용자 인증 코드 입력(Auth Code)

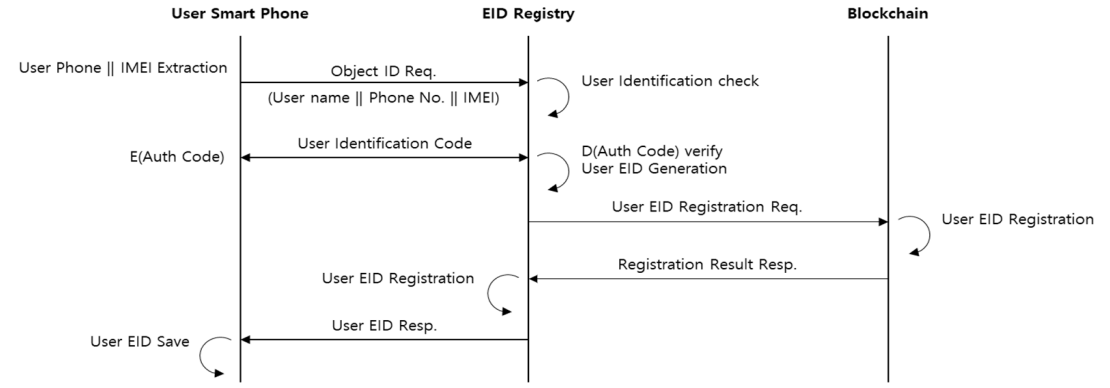

Fig. 3. User EID issue

③ 인증 코드 확인 및 EID 생성
④ EID 블록체인에 저장
⑤ EID 사용자에게 전송
⑥ 발급 완료

사용자 EID 발급 방법은 다음 Eq. (1)과 같다.

$$User\,EID = SHA256(issuing\,Auth\,Code \| User\,Smart\,Phone\,IMEI \| \times tamp) \quad (1)$$

EID 발급은 허가된 기관에서만 발급이 가능하며 발급 시 발급 기관 인증코드가 사용된다. 발급 기관 인증코드는 사용자마다 다르며, 발급된 사용자 인증코드는 블록체인에 저장한다. 블록체인에 저장되는 정보는 다음 Eq. (2)와 같다.

$$User\,Auth\_Code = (issuer\,ID \| issuing\,Auth\,Code \| User\,EID) \quad (2)$$

블록체인은 퍼블릭, 프라이빗, 컨소시엄 블록체인 등이 있으며, 중요 정보는 프라이빗 또는 컨소시엄 블록체인으로 구성할 것을 권장한다.

3.2 객체 EID 발급

객체 EID는 객체 제작 시 발급되어 Active Tag에 저장된다. 저장된 객체 EID는 객체가 판매되는 시점에서 사용자의 EID와 객체 EID를 접목하여 블록체인에 저장한다.

객체 EID 발급을 위해서는 객체에 대한 시리얼넘버와 제작사 고유값이 사용된다. 객체 EID 발급 방법은 다음 Eq. (3)과 같다.

$$Object\,EID = SHA256(Company\,ID \| Object\,Serial\,No) \quad (3)$$

발급된 객체 EID는 컨소시엄 블록체인에 저장하여 관리한다.

3.3 객체 추적

객체 추적을 위해서는 IoT 센서 위치 정보와 객체에 내장된 Active Tag를 통한 위치 정보를 활용한다. 또는 사용자의 스마트폰 설정에서 위치정보 사용을 허용한 경우 스마트폰 위치기반 서비스를 이용할 수 있다. 다음 Fig. 4는 객체 추적을 위한 전체 플로우를 나타낸다.

객체 추적을 위해서는 사용자와 IoT 센서의 상호인증을 통해 신뢰할 수 있는 IoT 센서에만 위치정보를 전송한다. 객체 추적을 위한 절차는 다음과 같다.

① IoT 센서에서 객체 또는 스마트폰 위치 정보 요청 (IoT Sensor ID 전송)
② 객체 EID 또는 사용자 EID 관제센터에 전송
③ 관제센터에서는 IoT 센서 ID를 검증하고 객체 또는 사용자 정보를 블록체인을 통해 확인
④ 관제센터에서는 검증 정보를 사용자에게 전송
⑤ 관제센터에 객체 EID와 위치정보 전송
⑥ 관제센터에서는 객체 EID와 위치정보 수신 후 기록
⑦ 객체 위치 정보 또는 사용자 스마트폰 위치정보를 IoT 센서에서 주기적으로 요청하여 수신

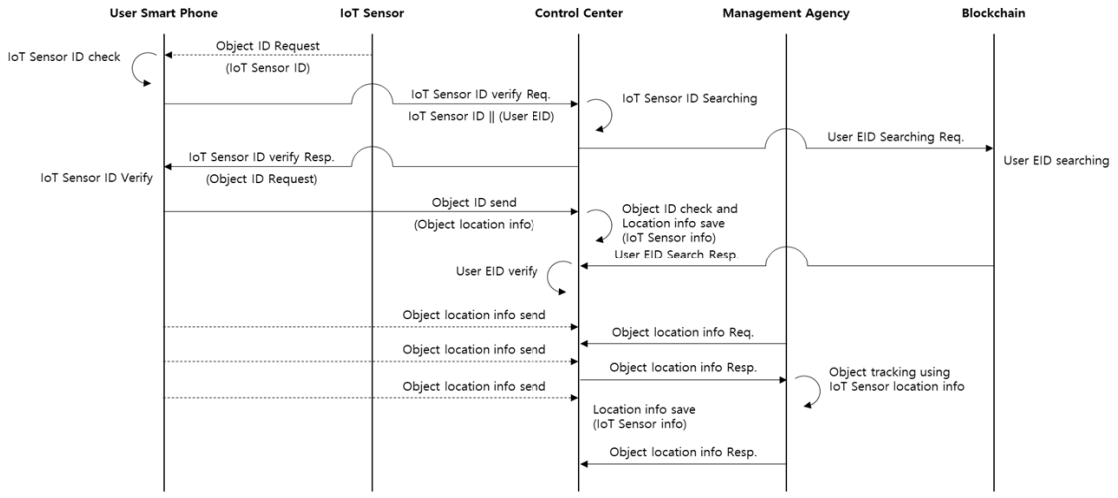

Fig. 4. Object trace

객체 또는 사용자 스마트폰에서 전송되는 정보는 다음 Eq. (4)과 같다.

$$Object location = Object EID \text{or } User EID \| location) \quad (4)$$

3.4 고지서 발송

고지서 발송은 사용자가 공유 자전거, 전동식 퀵보드, 공유 자동차 등을 이용하여 이동 중 위법 사항이 발생한 경우 등록된 스마트폰으로 사용자에게 발급된다. 고지서 발급에 대한 전체 플로우는 다음 Fig. 5와 같다.

고시서 발급에 필요한 정보는 사용자 EID, 객체 EID, 위법 영상, 관리기관 정보가 필요하며, 고지서 발급 정보는 다음 Eq. (5)와 같다.

$$Penaltybill = (User EID \| Agency ID \| \times tamp), movie \quad (5)$$

발급된 고지서는 인터넷뱅킹, 모바일뱅킹, 납부 전용 앱을 통해 스마트폰 또는 컴퓨터로 납부가 가능하다.

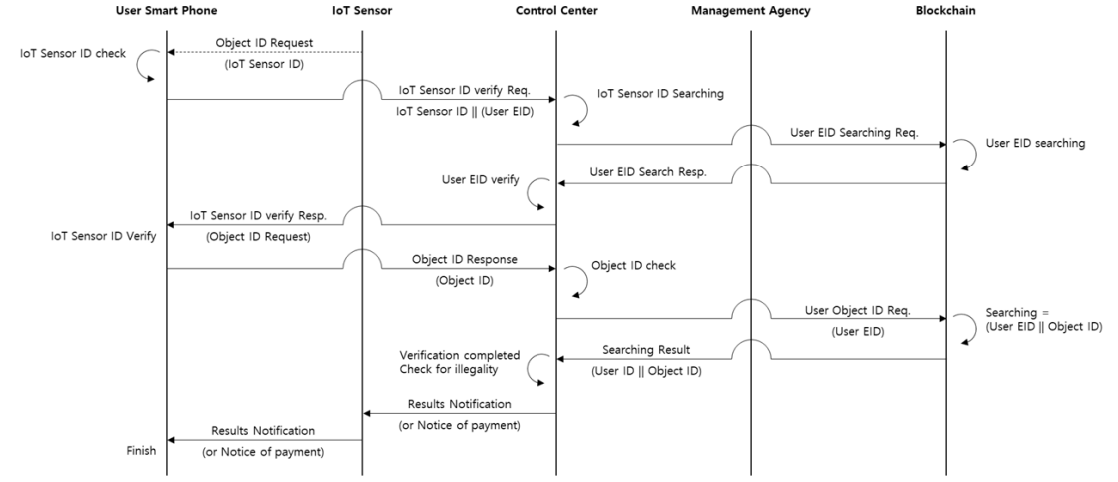

Fig. 5. notice issue

4. 실험 평가

제안하는 시스템의 성능 확인은 EID 안전성을 위주로 하였으며, 다양한 컴퓨팅 환경에서 발생하는 공격과 보안 침해 요소를 위주로 타 시스템과의 안전성을 비교 분석하였다.

4.1 보안성

제안하는 시스템에서 발급되는 모든 EID에 대한 안전성 확인을 위해 EID 안전성 및 무결성, Replay Attack 등을 사용하였다.

사용자 EID와 객체 EID 안전성 및 무결성을 위해 발급된 정보는 컨소시엄 블록체인에 저장한다. 블록체인 기술은 탈중앙화 속성으로 악의적인 해커로부터 안전하게 데이터를 보호할 수 있다.

또한 발급된 사용자 EID는 사용자의 휴대폰과 블록체인에 함께 저장되므로 위·변조가 불가능하므로 데이터의 무결성을 보증할 수 있다.

사용자 EID와 객체 EID 발급 시 발급기관에서 인증코드(Auth Code)와 challenge 값을 이용하여 발급에 대한 안전성을 고려하였으며, 발급된 EID 안전성을 위해 사용 시 본인확인을 필수로 한다.

블록체인 기술은 정보를 분산하여 저장함으로써 악의적인 공격자로부터 공격 포인트가 늘어나기 때문에 효율성이 떨어진다. 모든 암호화와 복호화는 사용자 휴대폰에서 이루어지므로 악의적인 공격자가 정보를 획득하여도 조합 알고리즘과 복호화키를 획득하지 못한다면 의미없는 정보가 된다. 그러므로 스니핑 공격과 재사용 공격으로부터 안전한다.

Table 1. Safety comparison

	A	B	Proposal
Storage location	Server	USB or computer	blockchain
safety	-	normal	safety
Replay attack	weak	safety	safety
sniffing	safety	safety	safety

4.2 편의성 및 확장성

제안하는 시스템은 사용자가 항상 휴대하는 스마트폰을 기반으로 EID를 발급하고, 발급된 EID를 이용하여 전동식 퀵보드, 공유 자전거, 카쉐어링 등을 이용 시 간편인증 서비스를 제공할 수 있다. 또한 발급된 EID와 객체(전동식 퀵보드, 공유 자전거, 카쉐어링 등)에 발급된 EID를 이용하여 위치 추적 및 위법 시 고지서 발급이 가능하도록 설계하였다.

제안하는 시스템은 확장성을 고려하여 설계하였으며, 기존 어떤 서비스와도 최소한의 변경으로 서비스 이용이 가능하다. 기존 서비스에 제안하는 시스템을 사용하기 위해서는 시스템 간 연동을 위한 프로그램 설치만 필요하다.

5. 결론

최근 개인 모빌리티 산업이 활성화되면서 다양한 사고가 발생하고 있다. 개인 모빌리티 산업은 개인이 편의성과 저렴한 비용으로 사용이 가능하여 많은 사용자들이 사용하고 있다. 하지만 개인 모빌리티 산업은 개인에게 편의성을 제공하지만 서비스 이용 시 본인확인 미흡과 사고 발생 시 책임소재에 대한 문제점이 대두되고 있다.

또한 서비스 이용 반납 시 정해진 장소 또는 무단 방치하여 2차 사고도 많이 발생하고 있다. 2차 사고 발생 시 책임소재가 불분명하여 모빌리티 서비스 제공 업체에 책임이 있다고 판단되지만 이 또한 모호한 기준으로 보상을 받기는 매우 어렵다.

제안하는 시스템에서는 모빌리티 산업의 발전을 위해 사용자와 객체에 EID를 발급하고 이를 이용하여 서비스 이용 시 사용자와 객체를 하나로 생각할 수 있는 방법으로 서비스 이용 시점부터 서비스 반납까지 전구간 추적이 가능하도록 하였다.

또한 서비스 이용 시 발생할 수 있는 위법 행위와 객체 도난 시 추적이 가능한 시스템을 제안하였다.

향후 AI를 연계하여 객체에 대한 비정상 행위를 추적할 수 있도록 개선할 것이며, 다양한 분야에 접목 가능할 수 있도록 개선할 것이다.

References

[1] FINANCIAL SECURITY INSTITUTE, “Electronic Finance and Financial Security No. 22”, Periodicals, FINANCIAL SECURITY INSTITUTE, Korea, pp97-110.

[2] 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.

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

[4] 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

[5] Sang-Il Choi, "Implementation of Service Model for Data-Driven Integrated Urban Management Service Operation Using Blockchain Technology", The Journal of The Korea Academia Industrial, Vol.20, No.10, pp.503-514, 2019.
DOI: https://doi.org/10.5762/KAIS.2019.20.10.503

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

[7] 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

[8] Jung Yong-hoon, "Blockchain-based new identification system", Journal of the Korea Academia-Industrial cooperation Society, Vol. 22, No. 2 pp. 452-458, 2021.
DOI: https://doi.org/10.5762/KAIS.2021.22.2.452

[9] Kwang-hyoung lee, Yong-hoon, "Blockchain-based safety MyData Service Model", Journal of the Korea Academia-Industrial cooperation Society, Vol. 21, No. 12, pp. 873-879, 2020.
DOI: https://doi.org/10.5762/KAIS.2020.21.12.873

[10] W3C Working Draft "Decentralized Identifiers (DIDs) v1.0", 19 July 2022, https://www.w3.org/TR/did-core/

이 광 형(Kwang-Hyoung Lee) [종신회원]

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

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

정 용 훈 (Young-Hoon Jung) [종신회원]

- 2006년 8월 : 숭실대학교 일반대학원 컴퓨터학과 (공학석사)
- 2010년 2월 : 숭실대학교 일반대학원 컴퓨터학과 (공학박사)
- 2011년 3월 ~ 2014년 2월 : 서일대학교 조교수
- 2018년 8월 ~ 2021년 3월 : 바스랩 연구소장
- 2021년 4월 ~ 현재 : 유니허브랩 연구소장

〈관심분야〉
블록체인, DID, 사용자 인증, 네트워크 보안, 융합 보안, AI