

블록체인 기반 출입통제 및 자재관리 시스템

이광형¹, 정용훈^{2*}

¹서일대학교 소프트웨어공학과, ²유니허브랩

Blockchain-based access control and material management system

Kwang Hyoung Lee¹, Yong Hoon Jung^{2*}

¹Department of Software Engineering, Seoil University

²UniHubLAB

요약 4차 산업혁명 시대에서는 블록체인, 인공지능, 빅데이터 등 정보에 대한 활용가치와 중요성이 높아지고 다양한 분야에 적용하고 있으며, 사용자 인증을 위한 정보를 최소화하는 기술로 변화하고 있다. 자재관리 분야에서는 고가의 자재 분실 방지를 위해 종이 대장을 통해 관리하고 있으나 미작성 및 허위 사실 기입으로 인한 한계가 발생하고 있다. 본 논문에서는 블록체인 기반 사용자 ID와 장비 ID를 발급하고 이를 통해 출입통제와 자재 관리 대장을 작성하여 블록체인에 분산 저장함으로써 허위사실에 대한 문제점을 해결하였다. 사용자 ID는 사원번호를 대체할 수 있으며, 공인인증서를 활용한 전자서명 또한 발급이 가능하다. 장비 ID는 재고 관리 및 분실, 재가공에 활용할 수 있도록 설계하였으며, 향후 자동 주문을 할 수 있도록 하였다. 제안하는 시스템에서는 블록체인에 제한이 없고, 사용자 단말기에 제한 없이 사용이 가능하다. 또한 사용자 개인정보를 수집하지 않으므로 개인정보 유출에 대한 문제점을 해결할 수 있다. 기존 시스템과 보안성, 무결성, 가용성, 편의성, 확장성을 비교하였으며, 다양한 공격방법과 휴대성, 대리 사용 등을 비교하여 우수함을 입증할 수 있었다.

Abstract In the era of the 4th industrial revolution, the value and importance of information in technologies such as blockchain, artificial intelligence, and big data is increasing, and the same is felt in various other fields. This situation is also growing positively to minimize information for user authentication. In material management, paper ledgers are used to prevent the loss of expensive materials, but there are limitations in this method due to the incomplete or false information provided. In this paper, the problem of false information was solved by issuing blockchain-based user IDs and equipment IDs, creating access control and material management ledgers, and storing them in a distributed manner in the blockchain. In the proposed system, a user ID can replace an employee number, and a digital signature using public certificate can also be issued. The equipment ID is designed to be used for inventory management, loss, and reprocessing, and hence automatic orders can be placed in the future. In the proposed system, there are no restrictions on the blockchain, and it can be used without restrictions on user terminals. In addition, since the user's personal information is not collected, the problem of personal information leakage is prevented. The existing system's security, integrity, convenience, and scalability were compared, and various attack methods, portability, and proxy use were compared to prove the proposed system's superiority.

Keywords : Blockchain, Authentication, Digital Signature, Identification. User ID

본 논문은 2021년도 서일대학교 학술연구비에 의해 연구되었음.

*Corresponding Author : Yong-Hoon Jung(UniHubLAB)

email: jung7773@naver.com

Received October 5, 2021

Accepted November 5, 2021

Revised October 15, 2021

Published November 30, 2021

1. 서론

최근 4차 산업혁명 시대에서 블록체인 기술, 인공지능, 빅데이터 등의 기술이 중요시 되고 있다. 블록체인 기술은 다양한 분야에서 인증, 이력관리 등에 사용되고 있다. 4차 산업혁명 시대에서는 정보의 중요성이 매우 높고 그에 대한 활용 가치가 높아 이를 빅데이터 기술을 연구하는 분야에서는 정보에 대한 처리 기술 및 활용 기술에 대해 많은 연구가 이루어지고 있다. 빅데이터 기술은 인공지능 기술과 결합하여 시너지효과를 낼 것으로 기대되고 있다. 기존 사용자 인증 및 접근제어 방식으로는 ID/PW, RF카드, 인증서, FIDO(생체인증) 등이 주로 사용되고 있다. 이러한 방법은 분실 시 불법 사용 및 위임, 재사용 등에 대한 문제점을 가지고 있다.

최근 출입통제를 위해 생체기반 인증 방식을 적용하고 있으나, 상황에 따라 인식이 불가능한 문제점을 가지고 있어 모바일 또는 기존 RF 카드 방식을 주로 사용하고 있다. 최근 휴대폰을 기반으로 FIDO 기술이 널리 사용되고 있으나 FIDO 기술은 비밀번호 대체 수단으로 휴대폰 분실 시 불법 사용과 생체 인식이 불가능한 문제점을 가지고 있다.

제안하는 블록체인 기반 출입통제 및 자재관리 시스템에서는 새로운 사용자 ID와 자재 ID를 발급하여 출입통제 및 자재관리 방법을 제안한다. 제안하는 시스템은 사용자 인증 및 출입통제 시 일회성 정보를 발급하여 재사용이 불가능하도록 설계하여 기존 문제점을 해결하였다. 또한 출입통제 및 자재대여에 대한 기록을 블록체인에 저장함으로써 전자문서에 대한 무결성 확보하였다. 제안하는 시스템에서 출입통제를 위해 사용된 사용자 본인확인 기술은 그룹웨어, ERP, MES, 웹사이트 등 다양한 분야에 활용 가능하도록 확장성을 고려하여 설계하였다. 3장에서는 제안하는 시스템에서 사용되는 사용자 ID, 자재 ID, 출입통제, 자재관리 방법 등을 기술한다. 4장에서 제안하는 시스템에 대한 보안성, 무결성, 가용성, 편의성, 확장성을 기준으로 기존 시스템과 비교 분석을 통해 우수함을 입증하였다[3].

2. 관련연구

2.1 기존 출입통제 시스템

기존 출입통제 시스템은 RFID를 주로 이용하고 있으며, 중앙 관리 서버, 개폐기, 인증 단말, RFID 카드로 구

성된다. RFID 카드 방식은 구성원에게 발급하는 카드와 방문자를 위한 임시 출입 카드를 구분된다. RFID 카드 방식은 지문인식이 가능한 카드 진화하여 사용되고 있으나, 배터리 충전 문제와 인식을 저하, 지문 복제, 분실로 인한 불법 사용 등의 문제점을 가지고 있다[2].

2.1.1 모바일 앱 기반의 출입통제 시스템

모바일 앱 기반의 출입통제 시스템에서는 기존 RF 카드 방식을 모바일 앱으로 구현한 인증 방식으로 NFC(Near Field Communication) 통신방식을 이용한다. NFC는 비접촉식 근거리 무선 통신기술로 두 단말기간 10cm 이내의 거리에서 데이터를 양방향으로 통신할 수 있는 기술이다.

모바일 앱 기반 출입통제 시스템은 FIDO 기술과 함께 사용한 방식으로 진화하였으나, 모바일에서 사용되고 있는 생체인증 기술인 FIDO 기술은 비밀번호 대체 수단으로 생체인증 실패 시 비밀번호를 이용하여 사용이 가능한 문제점을 가지고 있다[2].

2.1 블록체인

블록체인은 공공 거래 장부로 불리는 데이터 분산 처리기술을 의미하며, 블록체인 네트워크에 참여하는 모든 사용자가 모든 거래 내역 등의 데이터를 분산, 저장하는 기술이다. 블록체인에서 블록은 개인 간 거래 데이터가 기록되는 장부를 의미한다. 이런 블록들은 생성 후 시간의 흐름에 따라 순차적으로 연결된 구조를 가진다[1].

거래내역은 모든 사용자가 보유하고 있어 거래 내역을 확인할 때는 모든 사용자가 보유한 장부를 대조하고 확인 한다. 기존 거래 방식에서는 중앙 서버에 모든 정보를 보관하므로 공격에 취약하고, 데이터 위변조가 가능하다. 블록체인 기술은 데이터를 여러 명이 같은 정보를 저장하고 있기 때문에 위변조가 어렵다는 특징을 가진다. 블록체인 정보를 위변조하기 위해서는 참여자의 거래 데이터 모두를 수정해야하기 때문에 해킹은 불가능하다[4,7].

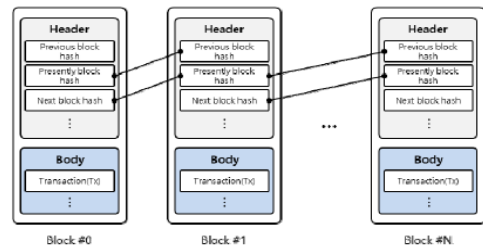


Fig. 1. Blockchain Structure

최근 블록체인 기반 사용자 인증 등에 관한 연구가 활발하게 진행되고 있다. 여러 민간 기업들은 DID 얼라이언스를 출범하고 분산ID(DID) 제품을 출시하고 있으며, 대학 및 연구소에서는 논문을 통해 발표되고 있다[1-6]. 또한 정부 기관에서도 블록체인 기반 기술에 대한 관심이 집중되고 있으며, 시범사업을 통해 일부 기관에서 DID 기반 신분증 사업을 채택하여 운영하고 있다.

2.2 사용자 인증

사용자 인증 방법은 ID/PW, 공인인증서, 생체인증, PIN 등을 가장 많이 사용하고 있으며, 최근에는 생체정보, 분산 ID 등을 이용한 인증 기술이 활발하게 연구되고 있으며, 다양한 분야에 적용되어 사용되고 있다[5].

2.2.1 PKI(Public Key Infrastructure)

인터넷이나 인트라넷 상의 사용자들에게 보안 서비스를 제공하는 체계로 국가 공개키 기반구조(NPKI, National Public Key Infrastructure)를 따르고 있다.

최상위 인증기관은 한국인터넷진흥원(KISA)에서 역할을 하고 있으며, 하위에는 5개의 인증기관(CA, Certificate Authority)이 있다. 인증기관은 한국인터넷진흥원을 대행하여 인증서 발급 및 재발급 서비스를 제공한다. 인증기관 하위에는 공인인증서의 접수 및 등록 등의 일을 대행하는 은행, 증권사와 같은 등록대행기관(RA)이 존재한다[1,9].

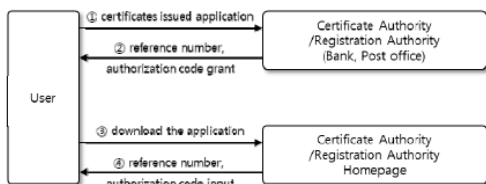


Fig. 2. Issuing Certificates

사용자들은 인증기관 또는 은행, 증권사에서 인증서를 발급 및 재발급 받을 수 있다.

인증서는 인터넷상에서 전자거래 등을 안심하게 사용할 수 있도록 해주는 사이버 증명서로 인감증명서와 비유할 수 있다. 인증서로 전자서명을 하면 상대방이 서명한 사람이 누구인지를 확인할 수 있으며, 전자문서의 위조나 변조 예방 및 거래 사실을 증명할 수 있다[1,9].

2.3 DID(Decentralized Identifier)

DID는 DID 주체와 관련된 URL로써, DID문서라는 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[8-10].

기존 연구에서는 W3C Working group 표준화를 응용한 새로운 신원확인체계에 대한 연구가 진행되었다. 기존 연구에서는 DID 발급을 위해 블록체인 계정(Account)과 발급기관에 대한 전자서명을 활용하여 DID를 발급하고 있다[1].

3. 본론

본 논문에서는 블록체인을 기반으로 한 신원확인, 출입통제 및 자재관리 시스템을 제안한다. 제안하는 시스템에서는 사용자 신원확인 및 출입통제를 위해 분산ID를 발급하고, 자재관리를 위해 자체별 ID를 부여하여 자재관리 및 분출대장을 블록체인에 저장하여 무결성을 확보하였다. 제안하는 시스템은 출고관리 클라이언트와 서버, 데시보드로 구성된다.

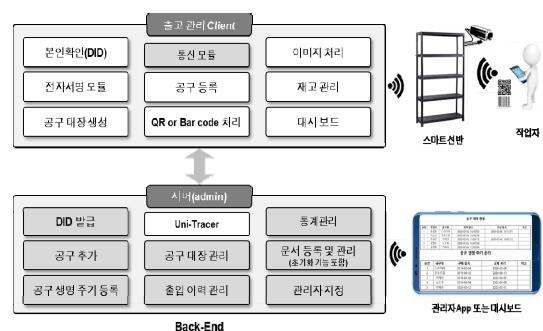


Fig. 3. Proposed system

블록체인은 용도에 따라 프라이빗(Private), 퍼블릭(Public), 컨소시엄(Consortium)으로 선택적으로 구성이 가능하다. 만약 본사와 많은 지사가 존재하는 경우 컨소시엄 블록체인 형태로 구성하여 허가된 구성원만 블록

을 생성할 수 있도록 한다. 제안하는 시스템에서는 컨소시엄 형태의 블록체인과 위임 지분 증명(DPoS) 방식을 이용하였다.

3.1 블록체인

블록체인은 분산ID와 출입통제 기록, 분출대장 등을 저장하는 용도로 사용된다. 본 논문에서는 컨소시엄 블록체인을 구성하여 본사와 지사에 인사 담당자가 분산ID를 발급하고 등록할 수 있도록 한다.

자재관리를 위한 자재 ID, 분출대장, 자재 라이프사이클, 이미지, 작업 일지 등을 위한 블록체인과 분산ID 등록 및 검증 정보와 출입대장 저장을 위한 블록체인을 별도로 관리한다. 합의 알고리즘은 컨소시엄에 적합하고 속도가 빠른 DPoS 방식을 사용하였으며, 합의 알고리즘에 대한 제한은 없다.

제안하는 시스템은 사용자의 분산ID를 이용하여 출입통제 구역에 대한 출입대장을 위변조가 불가능한 형태로 관리가 가능하다. 분산ID와 자재별ID를 이용하여 분출대장을 관리하여 자재 분실에 대한 문제점 해결이 가능하다.

3.2 접근제어

사용자 접근 제어를 위해 사용자 분산ID와 생체인증을 통해 등록된 AP와 등록된 디바이스에서만 인증을 통해 출입이 가능하다.

출입대장은 사용자의 분산ID와 전자서명을 통해 형식에 맞게 자동으로 작성된다. 출입대장에는 기본적으로 “년월일시분초”, “분산ID”, “전자서명”을 기록하지만 형식에는 제한이 없다.

출입대장 기록(Access Control List, ACL)에 저장되는 사용자 전자서명은 다음 식(1)과 같다.

$$ACL = User\ ID\ \| \ User_{DS}(User\ ID\ \| \ Time)\ \| \ Time \quad (1)$$

How to create a user electronic signature stored in the access log record

3.3 출고관리 클라이언트

장비대여를 위해서는 1차적으로 사용자 분산ID를 이용한 접근제어 이후 가능하다. 장비대여를 위해 출고관리 클라이언트에 등록된 사용자 분산ID와 접근제어에 입력된 사용자 분산ID를 비교하여 2차 신원확인 후 장비대여

가 가능하다.

출고관리 클라이언트에서는 장비 입출고 관리 및 공구 교체 관리, 장비 인식 기능을 수행한다. 장비 인식은 QR 코드 또는 바코드, 이미지 처리 등을 이용할 수 있다.

장비 대여 시에는 장비 ID와 사용자 ID와 전자서명이 함께 장비대여 목록에 작성된다. 장비 대여 대장(Equipment Rent List, ERL)에 기록되는 정보는 다음 식(2)와 같다.

$$ERL = Equipment\ ID\ \| \ User\ ID\ \| \ User_{DS}(User\ ID\ \| \ Equipment\ ID\ \| \ Time)\ \| \ Time \quad (2)$$

How to create the information recorded in the equipment rental ledger

3.4 서버

서버에서는 사용자 분산ID 등록 및 관리 장비 ID 등록 및 관리, 공구 라이프 사이클 등록 및 관리, 출입이력 관리, 대장 등록 관리 등을 처리한다. 출입이력, 장비 대장은 정해진 형식은 없으며 현장 상황에 따라 변동이 가능하다.

사용자 분산 ID 생성과 장비 ID 등록 시 서버에서는 Salt(Nonce)값을 생성하여 사용자 앱(App)으로 전송한다. 장비 ID 생성은 서버에서 생성되며, 관리자 전자서명을 포함하여 생성한다. 장비 ID(Equipment ID, EID)는 생성 식(3)과 같다.

$$EID = HMAC(Serial\ No\ \| \ Salt)\ \| \ Manager_{DS}(User\ ID\ \| \ Serial\ No)\ \| \ Serial\ No \quad (3)$$

How to create a device ID

사용자 인증 요청 시 서버에서는 사용자 분산 ID와 전자서명, 디바이스 정보를 이용하여 인증한다. 사용자 전자서명 검증은 블록체인에 등록된 공개키를 이용한다.

3.5 사용자

사용자는 휴대폰에 앱(App)을 설치하고, 설치된 앱에서는 사용자 ID, 전자서명 등을 생성할 수 있다. 사용자 ID 생성을 위해서는 서버에서 발급된 사원번호와 발급 승인 정보(Salt(Nonce)값)이 필요하다.

사용자 ID 발급 및 등록 절차는 다음과 같다.

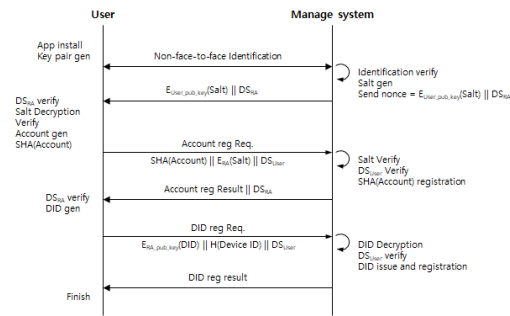


Fig. 4. User ID issuance procedure

사용자 앱에서는 분산 ID와 키쌍을 생성하여 본인확인, 전자서명 사용 시에 사용된다. 사용자 ID 생성은 다음 식(4)와 같다.

$$User ID = SHA(Employee IDNumber || Device ID || Salt) \quad (4)$$

How to create a user ID

전자서명은 상황에 따라 전자서명 생성 정보가 서로 다르다. 전자서명은 전자결제, 근태 관리, 출고 관리, 출입통제 등에 사용될 수 있다.

사용자 분산 ID 검증은 사용자 앱을 통해 전자서명을 생성하고, 전자서명 검증은 블록체인에 등록된 공개키를 이용하여 검증한다.

4. 성능분석

성능 분석에서는 보안성과 무결성, 가용성을 중심으로 하였으며, 편의성과 확장성을 추가로 고려하였다.

4.1 보안성

현재 사용자 본인확인 기술은 대부분 사용자의 정보를 중앙에서 생성 및 관리하기 때문에 악의적인 사용자의 공격에 노출되어 있다.

제안하는 시스템에서는 블록체인 기술과 사용자 중심의 정보 저장 방식을 이용하여 정보를 분산함으로써 공격에 대한 효율성이 떨어진다.

또한 악의적인 사용자가 공격을 통해 개인정보 또는 본인확인 정보를 획득하더라도 한 사람의 정보를 획득하기 위해 많은 시간과 노력을 투자해야 한다.

Table 1. comparison of authentication techniques

	safety	convenience
PIN	lowness	height
OTP	height	lowness
Certificate	height	lowness
FIDO	height	middle
Proposal	height	height

FIDO 기술을 사용하기 위해서는 생체를 지원하는 단말기에 제한된다. 하지만 제안하는 시스템에서는 단말기가 생체정보를 지원하지 않아도 사용이 가능하다. 획득한 정보를 사용 가능한 정보로 만들기 위해서는 생체 알고리즘과 암호화 방법을 모를 경우 의미 없는 정보라 할 수 있다.

Table 2. Safety comparison

	Certification	Proposal
Management entity	User	User
Copy	○	X
Steal	○	X
man in the middle attack	○	X

4.2 무결성

정보의 무결성을 보장하기 위해 해시 알고리즘을 사용하여 암호화하는 경우가 일반적이다. 제안하는 시스템에서는 전자문서에 대한 무결성 보장을 위해 블록체인 기술을 사용하였으며, 추가적으로 부인방지를 위해 전자서명 기술을 사용하였다.

제안하는 시스템에서 사용되는 전자서명은 소유 기반의 사용자 휴대폰에서만 생성 가능하며, 사용 목적에 따라 서로 다른 전자서명을 사용한다. 전자서명은 사용 목적에 따라 정보가 다르며, 생성 시간 정보를 포함하여 재사용이 불가능하도록 설계되었다. 또한 보안성과 무결성을 고려하여 합의 규약을 통한 이중기재 방지 기능을 추가하였다.

4.3 가용성

가용성 테스트를 위해 특정 노드에 장애가 발생하여 접속이 불가능 경우 서비스 지속 여부를 테스트 하였다. 추가적으로 블록체인에 대한 시스템 효율성을 위해 다수의 사용자가 동시에 접속하여 데이터 등록 요청을 할 경우를 가정하여 평균 성능(TPS)을 측정하고 테스트를 진

행하였다.

테스트 스크립트를 이용하여 모든 노드가 정상 운영되었을 때의 결과값을 수집 보관한다. 이후 특정 노드를 차단하고 스크립트를 수행하여 이전 결과값과 비교하여 이상 여부를 확인하였다.

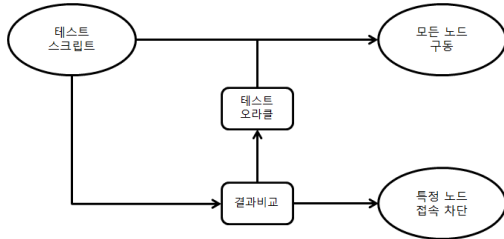


Fig. 5. Test method

블록체인 노드에서는 블록생성, 검증, 조회 등 여러 가지 역할을 나누어 수행할 수 있기 때문에 접속을 차단하는 노드를 특성에 맞게 선택해야 한다. 단 합의 알고리즘이 성공하기 위한 조건 2/3 이상의 블록 생성자가 활성화 되도록 접속 차단 노드를 유지하며 테스트를 하였다. 블록 생성 권한을 가진 노드에 장애 발생 시 블록생성 권한이 다른 노드로 이양되게 하여 신규 블록생성 및 검증이 정상적으로 수행되는 것을 확인하였다. 또한 블록생성 권한이 없는 일반 노드 장애 발생 시 신규 블록생성 및 검증이 정상적으로 수행되는 것을 확인하였다.

4.4 편의성 및 확장성

제안하는 시스템에서 사용하는 본인확인을 위한 정보는 다양한 분야에서 사용 가능하도록 설계되었다. 사용자 편의성을 고려하여 전자결제, 출입통제, 출고관리, 본인확인 등 휴대폰만 소유하고 있으면 사용이 가능하다.

휴대폰에 전용 앱 설치 시 사용자 본인확인 및 전자서명 기능을 사용할 수 있으며, 추가인증 수단으로도 적용 가능하다. 대표적으로 적용 가능한 분야는 본인확인 및 전자서명 기술이 필요한 ERP, MES 등이 있다.

5. 결론

최근 비대면 본인확인 기술의 발달로 생체정보, 분산 ID 등 다양한 방법에 대한 연구가 활발하게 진행되고 있다. 또한 전자문서 활용도가 높아짐으로써 전자서명 기술에 대한 활용도가 높아지고 있다. 그러나 사용자의 개인

정보를 무분별하게 수집하여 위협에 노출되고 있으며, 중앙 서버에 보관 및 관리하기 위해 보안장비 및 보안인력에 많은 비용을 소비하고 있다.

제안하는 시스템에서는 블록체인 기술과 소유 기반의 본인확인 기술을 통해 유지비용을 최소화하고 보다 안전한 시스템을 제안하였다. 사용자의 본인확인 정보는 사용자 휴대폰에서 직접 발급되며, 관리자는 확인을 통해 사용자에게 본인확인 정보를 생성하기 위한 최소한의 정보만 제공한다.

향후 시스템의 기능 향상을 위해 실시간으로 촬영된 이미지와 등록된 이미지를 비교할 수 있는 이미지 검출(Image detection) 기술을 통해 출고관리 시스템 기능을 향상할 것이다. 또한 재고량 부족시 등록된 업체와 자동 주문 및 전자영수증 발급, 전자계약서 작성 등을 추가하여 사용자 편의성을 제공할 것이다.

References

- [1] 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>
- [2] 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>
- [3] Soon-Chul Baek, Hong, In-Sik, "Smart Entrance Control System Using Face Recognition and OTAC", Journal of Knowledge Information Technology and Systems, Vol.15, No.4, pp. 451-461, August. 2020.
DOI : <https://doi.org/10.34163/jikits.2020.15.4.001>
- [4] 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>
- [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/IJIBC.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] 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>
- [8] Security Technology Research Team, "Overseas Research Trends Related to Blockchain Interworking" FINANCIAL SECURITY INSTITUTE, Korea
- [9] FINANCIAL SECURITY INSTITUTE, "Electronic Finance and Financial Security No. 22", Periodicals, FINANCIAL SECURITY INSTITUTE, Korea, pp97~110
- [10] W3C Working Draft "Decentralized Identifiers (DIDs) v1.0", 14 July 2020,
-

이 광 형(Kwang-Hyoung Lee)

[중심회원]



- 1998년 2월 : 광주대학교 컴퓨터 공학과 졸업(공학사)
- 2002년 2월 : 송실대학교 컴퓨터 공학과 (공학석사)
- 2005년 2월 : 송실대학교 컴퓨터 공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학 소프트웨어공학과 정교수

<관심분야>

멀티미디어 데이터 검색, 영상처리, 멀티미디어 보안, 학습 콘텐츠, AI

정 용 훈(Yong-Hoon Jung)

[중심회원]



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

<관심분야>

블록체인, 사용자 인증, 네트워크 보안, 융합 보안