Journal of the Korea Academia-Industrial cooperation Society
Vol. 21, No. 3 pp. 24-31, 2020

https://doi.org/10.5762/KAIS.2020.21.3.24
ISSN 1975-4701 / eISSN 2288-4688

블록체인 환경에서 EID를 이용한 사용자 통합 인증 시스템

김재용[1], 정용훈[2*], 전문석[1], 이상범[2]
[1]숭실대학교 컴퓨터공학과, [2]유니허브랩

User Integrated Authentication System using EID in Blockchain Environment

Jai-Yong Kim[1], Yong-Hoon Jung[2*], Moon-Seog Jun[1], Sang-Beon Lee[2]
[1]Dept. of Computer Science, Soong-Sil University, [2]UniHubLAB

요 약 기존의 컴퓨팅 환경에서 사용되는 중앙 집중형 시스템은 해킹에 의한 개인정보 침해 사례와 시스템 장애 발생 시 가용성 침해 문제 등의 다양한 문제점을 가지고 있다. 현재 신뢰받는 차세대 융합 정보 핵심 기술 중 하나인 블록체인은 다양한 문제점을 가지고 있던 기존의 중앙 집중형 시스템의 대안 기술로 기대 되고 있으며, 블록체인 환경에 맞는 사용자 인증 시스템의 필요성이 증가 하고 있다. 본 논문은 온라인 환경에서 EID를 이용하여 사용자 식별이 가능한 블록체인 기반의 사용자 통합 인증 시스템을 제안한다. 기존 ID/PW 인증 방식은 사용자가 여러 사이트에 개인정보를 저장하고 각각의 ID를 발급 받아 사용해야 한다. 그러나 제안하는 시스템은 EID 발급 후 여러 사이트에서 회원가입 없이 사용이 가능하다. 제안 시스템은 이메일 및 전화번호 등 최소한의 정보로 EID를 발급한다. 기존 중앙 집중형 시스템과 제안하는 통합 인증 시스템의 안정성과 효율성을 비교하여 우수함을 입증하였다. 컴퓨팅 환경에서 발생하는 공격방법과 침해요소를 선택하여 기존 시스템과의 안정성을 비교 하였다. 또한 효율성의 검증을 위하여 인증과정에서 발생하는 사용자의 App, 발행 및 인증기관의 서버, 서비스 제공기관 서버 사이의 총 처리량을 트랜잭션 당 처리시간으로 비교 분석하였다.

Abstract Centralized systems in computing environments have various problems, such as privacy infringement due to hacking, and the possibility of privacy violations in case of system failure. Blockchain, one of the core technologies for the next generation of converged information, is expected to be an alternative to the existing centralized system, which has had various problems. This paper proposes a blockchain-based user authentication system that can identify users using EID in an online environment. Existing identification (ID)/password (PW) authentication methods require users to store personal information in multiple sites, and receive and use their respective IDs. However, the proposed system can be used without users signing up at various sites after the issuing of an EID. The proposed system issues an EID with a minimum of information, such as an e-mail address and a telephone number. By comparing the stability and efficiency of a centralized system, the proposed integrated authentication system proved to be excellent. In order to compare stability against existing systems, we chose attack methods and encroachments on the computing environment. To verify efficiency, the total throughput between the user's app, the issuance and certification-authority's servers, and the service provider's servers was compared and analyzed based on processing time per transaction.

Keywords : User Authentication, Identification, SSO, Block Chain, OTP

*Corresponding Author : Yong-Hoon Jung(Soong-Sil Univ.)
email: jung7773@naver.com
Received January 2, 2020 Revised February 17, 2020
Accepted March 6, 2020 Published March 31, 2020

1. 서론

컴퓨팅 환경이 활용되는 분야가 증가함에 따라 사용되는 개인정보의 활용가치와 중요성은 높아지고 있으며, 신원정보를 검증하는 사용자 인증 기술 역시 함께 발전하며 변화 하고 있다. 개인 정보를 여러 공간에 저장하고 사용하면서, 개인정보 침해 및 해킹 등의 보안사고 사례가 증가 하고 있다. 개인 정보를 제공하고 활용하는 방법에 대한 논의는 계속 되고 있다[1-3].

지금까지 산업 및 생활환경 등의 분야에서 활용되는 컴퓨팅 환경은 기존의 중앙 집중형 시스템에서 블록체인 기반의 분산 시스템 형태로 변화 하고 있다. 블록체인은 정보를 교환하는 모든 구성원이 인증된 제3자 기관의 개입 없이, 데이터를 공동으로 보관하는 분산장부에 저장 및 기록하는 기술이다. 블록체인은 현재 차세대 융합 정보 핵심 기술로서 다양한 분야에 활용 되고 있으며, 기존 중앙 집중형 컴퓨팅 환경을 대체 하는 기반 기술로 기대되고 있다[4-6].

컴퓨팅 환경이 블록체인 기반의 분산 시스템으로 변화함에 따라, 기존의 컴퓨팅 환경에서 적용되던 개인정보의 활용 방법과 사용자 인증 기술의 변화 역시 필요하게 되었다. 블록체인 환경이 다양한 영역에서 적용 되고 발전하면서, 블록체인 환경에 맞는 사용자 인증 기술과 개인정보 보호를 위한 대책이 필요하게 되었다.

기존 컴퓨팅 환경에서 사용하는 대표적인 사용자 인증 시스템은 ID/PW방식이다. 사용자를 식별 할 수 있는 ID와 매칭되는 PW를 중앙 서버 데이터베이스에 저장 하고, 사용자가 제시하는 ID/PW를 데이터베이스에 저장된 ID/PW와 비교하여 사용자를 식별 및 인증 한다. 온라인 환경에서 사용자 인증 시스템으로 활용되던 ID/PW 방식은 중앙 서버가 가지고 있는 취약점으로 많은 문제를 발생 시켰다. ID/PW 방식은 한 명의 사용자가 여러 사이트에 ID 등록을 위해 매번 등록과정을 진행해야 하는 번거로움이 있고, 여러 곳에 등록된 많은 계정들을 관리하는 어려움이 있었다. 또한 사용자의 개인정보를 너무 많은 저장소에 저장함으로서, 개인정보 침해 사고에 대한 위험성이 매우 높았다[7-9].

본 논문은 블록체인 환경에서 위변조 방지가 가능한 EID(Electronic ID)를 이용한 사용자 통합 인증 시스템을 제안한다. 여러 사이트에서 각각의 ID로 사용자의 신원을 확인하는 것과 달리, 하나의 EID로 여러 사이트에서 신원 정보의 확인과 검증이 가능하다. 사용자는 한번 발급한 EID로 온라인 환경에서 자신의 신원정보를 식별하고 검증 하는 전자 신분증으로 사용이 가능하다.

EID를 발급하기 위해 먼저 사용자 신원확인 과정이 필요하다. 이메일 및 전화번호를 이용한 인증 과정을 거치며 사용자에게 이름과 생일 등의 최소의 정보만 요구한다. 또한 발급 과정에서 제공하는 사용자의 정보는 중앙 집중형 시스템의 데이터베이스가 아닌, 블록체인 기반의 분산 노드에 안전하게 저장 된다. 사용자의 정보는 사용자의 개인키, 공개키 키쌍으로 관리되어 사용자 외에 누구에게도 공개되지 않는 완벽한 비밀성을 보장 받는다.

제안하는 사용자 통합 인증 시스템은 기존 ID/PW 방식에서 PW의 분실 및 유출에 대한 문제점을 보완하기 위하여, 스마트폰 애플리케이션을 이용한 인증 방식을 제안한다. 로그인 과정에서 사용자의 ID와 매칭되는 PW를 입력하는 과정 대신에 스마트폰에서 패턴, PIN, BIO 정보를 이용한 인증 방식을 지원한다. 사용자가 제시한 EID가 자신의 EID임을 인증하고, 제시한 EID의 유효성을 블록체인 기반의 분산 노드 시스템을 통해 검증 받는 과정을 거치게 된다.

또한 신원 정보의 검증 외에도 사용자가 참가하여 발생하는 다양한 형태의 거래에서 부인방지, 무결성 검증 및 위변조 방지기능도 함께 제공한다.

본 논문의 구성은 다음과 같다. 2장에서는 사용자 통합인증 시스템의 관련 연구에 대해 분석한다. 3장에서는 블록체인 환경에서 EID를 이용한 사용자 통합 인증 시스템을 제안하고, 4장에서 제안시스템의 성능분석에 대한 내용을 기술한다. 마지막 5장에서 결론으로 마무리한다.

2. 관련연구

2.1 사용자 인증

인터넷이 발전하면서, 컴퓨팅 환경을 통한 다양한 업무가 가능하게 되었다. 정보의 공유, 계약의 체결 등 상대방의 신원을 확실히 인증하고, 주고받는 데이터의 정확성을 확인하는 것이 필수적인 요소가 되었다. 사용자 인증(User Authentication)은 컴퓨팅 환경에서 거래 당사자 간에 상대의 신분을 검증하는 것(Identity Validation)을 말하며, 하나의 세션 동안에 거래 당사자(사람, 프로세스, 클라이언트, 서버 등)간에 상대의 주장하는 신원(Identify claim)에 대해 유효성을 성립시키는 것을 말한다[7].

사용자 인증방식은 인증하는 방식에 따라서, 지식 기반 인증과 소유기반 인증 그리고 특징 기반 인증으로 분

류 할 수 있다. 지식 기반 인증방식은 사람의 지식에 따른 내용으로 인증하는 방식으로 관리가 편하고 구축이 용이하다는 장점이 있다. 지식 기반 인증방식으로는 ID/PW, Passphrase, 사전 등록된 문답, i-Pin 등이 있다. 소유 기반 인증방식은 별도의 보안매체를 통해 고유정보를 제시하여 인증하는 방식으로 매체에 대한 분실 우려가 높다는 단점이 있다. 소유 기반 인증방식으로는 OTP, 보안카드, 공인인증서, HSM 등이 있다. 특징 기반 인증방식은 사용자의 생체특성이나 행동학적 특성을 통해 인증하는 방식이다. 대표적인 특징 기반 인증방식은 지문인식, 홍채 및 망막인식, 안면인식, 음성인식 등이 있다[8,9].

2.2 전자신분증의 보안 프로토콜

개인의 신원정보를 나타내는 신분증은 개인정보를 식별하고 확인하는 역할을 하며, 플라스틱 카드의 형태로 제작하여 소지한다. 기존의 플라스틱 신분증에 접촉식 스마트카드 기능의 IC칩을 추가 하여 전자 신분증이라고 하며, 주민등록번호, 지문정보, 공인인증서 등의 개인정보를 IC 칩에 저장하여 전산시스템에서 활용 하고 있다[10]. 전자신분증으로 사용되는 스마트카드는 개인식별(identification), 인증(authentication), 그리고 전자서명(digital signature)에 주로 사용되며, 기존의 오프라인에서 사용되는 신원 확인 정보를 대체하여 더욱 안전하고 신뢰성 있는 개인의 식별을 가능하게 하며, 온라인 환경에서도 일관성 있게 사용할 수 있다는 이점이 있다.

전자신분증에 활용되는 개인정보 보호를 위한 보안 프로토콜 표준은 전자여권 표준인 국제민간항공기구의 BAC(Basic Access Control), PA(Passive Authentication), AA(ActiveAuthentication)가 있다.

BAC는 전자신분증 칩에 저장된 데이터가 공격자에게 불법적으로 읽히는 것과 전자신분증 칩과 판독시스템 간에 전송되는 정보의 도청을 방지하는 접근통제 메커니즘이다. PA는 칩의 LDS(Logical Data Structure)에 포함되어 있는 정보가 수정되지 않았음을 알려주는 보안 메커니즘이다. 전자신분증 발행기관이 암호화 방식을 적용하여 전자신분증 내의 칩에 대한 정보를 저장하고, 해시(Hash)를 이용한 전자 서명을 통해 칩 안의 정보를 암호화한다[11-13].

2.3 블록체인과 개인정보 보호

국내 블록체인 기술 활용은 금융시장을 시작으로 다양한 분야에서 활용되고 있다. 은행 및 투자업계는 외화송금, 보험금 청구 서비스, 대출 등의 다양한 금융 서비스에 블록체인을 활용한 서비스를 시범운영 및 계획 하고 있다. 또한 국가 기반 사업 및 민간 서비스 기업에서도 블록체인을 활용한 서비스에 대한 활발한 참여와 연구가 진행 되고 있다[14-16].

블록체인 기술을 이용하는 비즈니스 모델 대부분이 개인정보의 처리과정이 필요하기 때문에, 블록체인의 탈중앙화 속성과 기존의 개인정보 보호법제 간에는 부합되지 않는 문제점이 존재하며 개선에 대한 필요성이 대두 되고 있다.

개인정보 보호법에서는 개인정보를 처리하는 공공기관, 법인, 단체 및 개인을 개인정보 처리자로 정의하고 있다. 블록체인에 참여한 업체 또는 기관들이 개인정보 처리자로서 개인정보의 수집·이용·제공·삭제·안전조치의무 등 개인정보 보호법상의 각종 의무를 준수하여야 한다[2].

국내 주요 개인정보 보호법제들은 모두 보유기간이 경과하거나 처리 목적이 달성된 개인정보는 파기하도록 정하고 있다. 그러나 블록체인에서 개인정보를 이용하는 경우에는 블록체인 데이터의 비가역성으로 인해 데이터의 삭제나 변조가 불가능하다.

3. 제안하는 시스템

제안하는 사용자 인증 시스템은 블록체인 환경에서 사용자에게 발급한 EID로 사용자의 신원을 확인 및 보증하고, 개인정보를 안전하게 보호 할 수 있는 방법을 제공한다.

3.1 시스템 구성요소

제안하는 시스템은 EID를 발급받아 사용하는 사용자(USER), EID를 발급하고 관리하는 EID Authentication System, EID로 사용자의 정보를 활용하는 Verifier(OSP), 블록체인 환경의 저장 스토리지로 구성이 되어 있다.

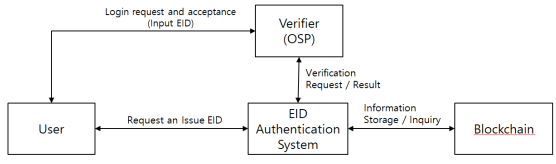

Fig. 1. Component of Authentication System

사용자는 EID를 발급받아 자신의 신원을 확인 할 수 있다. 사용자는 EID를 발급 받기 위해 이메일 및 SMS 인증 과정이 포함된 KYC(Know Your Customer)인증으로 자신의 신원을 증명해야 한다. EID 발급에 사용된 모든 정보는 비식별화 및 암호화 처리되어 블록체인 환경의 분산 노드에 분할 저장된다. 사용자는 Wallet 형태로 제공되는 DAPP(Decentralized Application)을 통해 EID를 발급 받고 사용하기 위한 인터페이스를 제공받는다.

EID Authentication System은 사용자(USER)와 Verifier(OSP)등에게 EID를 발급하고 관리하며, 블록체인 분산 노드의 운영에 대한 역할도 함께 수행한다. EID 발급을 위한 Serial Number를 생성하고, 생성한 Serial Number의 유효성을 검증하여 중복 생성을 방지한다. 또한 사용자가 DAPP에서 생성한 키쌍 중 공개키를 블록체인 분산 노드에 등록하고, 분산 스토리지에 데이터를 저장하거나 조회하는 역할을 수행한다.

Verifier(OSP)도 사용자 인증 시스템에 참여하기 위해 EID를 발급받아 사용 한다. 하지만 사용자와 달리 EID를 통해 신원 정보를 검증 한 사용자에게 로그인 기능을 제공하며, 별도의 서비스를 제공 하는 역할을 수행한다. 사용자가 제시한 EID로 사용자 신원정보에 대한 검증을 EID Authentication System에게 요청하며, 결과에 따라 사용자에게 서비스 제공 유무를 결정 한다.

블록체인 분산 스토리지는 사용자 인증 시스템에서 데이터를 저장하기 위한 공간으로 사용되며, 기존의 중앙집중형 시스템의 데이터베이스와 같은 역할을 한다. 하지만 데이터베이스와 달리 단일 시스템의 구조가 아닌 분산 노드의 형태로 구성되며, 데이터의 저장과 조회는 EID Authentication System을 통해서만 가능한 구조로 구성된다.

3.2 EID 구조 및 생성

3.2.1 EID 구조

EID는 개인을 식별하기 위한 ID의 역할을 하며, 16진수의 형태의 64byte로 구성된다. 또한 EID를 구성하는 필드는 Fig 2와 같다.

EID를 구성하기 위한 사용자의 정보는 이름, 생년월일, 이메일, 휴대폰 번호 등이 있으며, EID 발급을 위해서 반드시 필요하다.

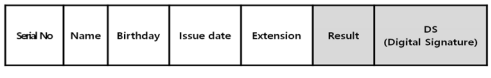

Fig. 2. Filed of EID

EID를 구성하는 각 필드의 세부 내용은 다음 Table 1과 같다.

Table 1. Field Characteristic of EID

Field	Characteristic
Serial No	발급 기관의 식별번호와 일련번호의 조합이며, 34bit(long Serial)로 사용된다.
Name	사용자의 이름으로 20byte(string name)로 사용된다.
Birthday	사용자 생년월일과 성별 정보이며, 8byte(int birth)로 사용된다.
Issue date	EID의 발급 일자이며, 8byte(int issue_date)로 사용된다.
Extension Field	전 세계의 각 국가별로 할당된 국가코드와 EID 발급을 위해 필요한 사용자의 휴대폰 번호(Phone No), E-mail, SMS or KYC등의 정보를 저장한다.

3.2.2 EID 생성

DAPP에서 생성한 EID는 QR 코드의 형태로 사용 할 수 있다. 사용자가 EID 발급을 요청하면, Serial NO와 사용자 정보를 결합하여 EID를 생성하고, EID 요청과 함께 생성한 OTP를 EID와 조합하여 QR 코드를 생성하여 전송한다. 발급된 EID 값은 변하지 않으며, 이미지 캡처, 위조, 위임 등을 막기 위해 OTP를 생성하여 EID와 결합하여 제공한다.

$$EID = SHA256(SerialNo \| Name \| Birthday(7digit) \| issuedate \| Extension) \quad (1)$$

$$QRcode = EID + OTP(\text{or } Randomnumber) \quad (2)$$

생성된 EID는 블록체인에 등록되며, EID 재발급을 위해 사용된다. EID 블록정보는 Fig 3과 같다.

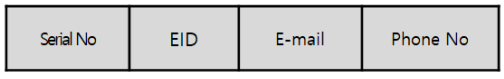

Fig. 3. EID Block

EID 발급은 블록을 생성하는 BP들의 합의에 의해 이루어진다. BP들은 SMS와 KYC 인증 여부 확인 후 찬성 또는 거부할 수 있으며, SMS와 KYC 인증 여부와 관계없이 BP들의 과반수 찬성으로 EID가 생성 될 수 있다.

EID 생성을 위해 모든 BP가 투표를 하고 마지막 BP는 최종적으로 모든 BP들의 서명을 모아 최종 전자서명한다. 서명된 데이터는 EID에 첨부된다. BP들에 순서는

정해진 것이 없으며, 먼저 처리된 결과가 순차적으로 쌓이게 된다.

$$Result = SHA256(BP1 \bullet DS \cdots BP21 \bullet DS), \\ E_{LastBPPrivateKey}[Hash(BP1 \bullet DS \cdots BP21 \bullet DS)] \quad (3)$$

3.2.3 QR code 생성

제안하는 시스템은 QR code 생성을 위하여, EID 값과 생성한 OTP값을 결합한다. QR code에 포함된 EID의 유효성 검증을 위해서 EID값에 포함되어 있는 OTP 값을 분리 한다. OTP는 EID값 특정 위치에 삽입되며, 삽입된 위치는 운영주체 시스템에서만 확인이 가능하다.

$$OTP = OTPgenerator(6digit) \quad (4)$$

$$QRcode = Add\ \ OTP\ value\ \ to\ \ EID\ random\ \ location \quad (5)$$

OTP값이 추가되는 위치는 OTP 두 자리가 EID에 추가될 위치와 추가되는 값이 된다. 단 63이상이면 한자리가 위치 값과 추가되는 값이 된다. 생성된 QR code는 정해진 시간 이후 사용이 불가능하다. 생성된 QR code는 일정 시간에만 유효성을 인정받을 수 있고, 정해진 시간 내에 1회에 한하여 인증 할 수 있다.

3.3 EID 발급 및 검증

3.3.1 EID 발급

사용자 인증 시스템에 참여하는 사용자와 OSP는 운영주체 시스템을 통해 EID를 발급 받아야 한다. 사용자와 OSP는 신원정보를 검증하는 인증 절차를 거친 후에 자신의 신원정보를 식별할 수 있는 EID의 사용과 검증을 요청 할 수 있다.

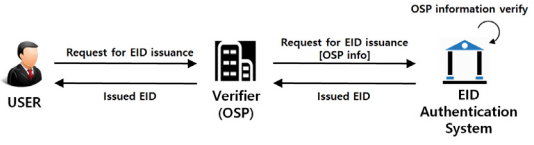

Fig. 4. EID Issuance Procedure

EID 발급 절차는 다음과 같다.

1) 최초 사용자와 OSP 는 운영주체 시스템을 통해 EID 발급 신청을 한다.
2) 운영주체 시스템은 사용자와 OSP가 제출하는 정보를 확인 하고 EID 생성 여부를 결정한다.
3) 생성 거부 메시지 또는 생성된 EID는 사용자, OSP에게 전달된다.

3.3.2 EID 검증

EID는 회원가입 없이 각각의 사이트에서 사용 할 수 있는 온라인 통합 신분증이 된다. EID는 OSP 사이트에 로그인하는 사용자의 신원정보를 증명하는 용도로만 사용된다. EID를 발급받은 사용자는 OSP에게 EID를 제시하고, 운영주체 시스템을 통해 검증 받은 결과로 OSP는 로그인 여부를 판단한다.

회원가입 없이 OSP가 제공하는 서비스를 이용하기 위해, 사용자는 웹 페이지에서 로그인을 요청 하며 EID를 전달한다. OSP 역시 EID를 발급받아 사용자 인증 시스템에 참여한 경우에만 사용자 EID의 검증 요청이 가능하며, 운영주체 시스템의 EID 검증 결과를 기다린다. 사용자가 OSP에게 EID 전송 할 때, 전자서명 값이 포함되어 함께 전송된다.

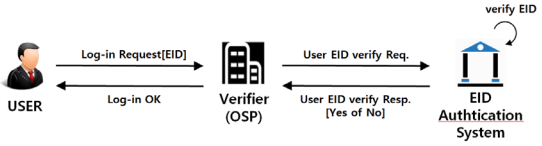

Fig. 5. Using EID

1) 서비스 이용 요청(EID 전송)
2) OSP는 자체 검증 또는 운영주체 시스템에게 EID 검증을 요청한다.
3) EID 검증 결과를 사용자에게 전달한다. Pass일 경우 사용자는 OSP 서비스 이용이 가능하다.
4) Login 완료

3.3.3 EID 재발급 및 폐기

운영주체 시스템은 EID 재발급 요청 시에 사용자 본인확인을 위해 등록된 이메일과 SMS을 이용한 인증 절차를 진행하고, 인증이 완료되면 사용자에게 EID를 재발급 한다. 운영주체 시스템은 사용자 이메일과 휴대폰 번호를 블록체인 분산 노드에서 검색하여 해당하는 EID를 조회한다. EID 조회를 위한 이메일과 휴대폰 번호는 SHA256(E-mail || Phone No)로 해쉬 처리되어 블록체인에서 검색한다. 운영주체 시스템은 사용자에게 EID를 재발급 하는 동시에 counter 값을 증가시키고,

Serial No와 함께 발급기관에서 별도 관리한다. EID 폐기는 사용자의 요청에 의해 이루어지며, 폐기 요청 시 폐기 목록을 관리하는 체인에 Serial No가 등록된다. 발급 정보를 관리하는 체인에서는 등록된 블록 정보를 삭제한다.

4. 성능분석

통합인증 시스템의 성능 확인은 안정성과 효율성 부분으로 구분하여 수행 하였다. 컴퓨팅 환경에서 발생하는 다양한 공격과 보안 침해 요소를 선택하여, 타 인증 시스템과의 안정성을 비교 분석 하였다. 또한 사용자 인증 과정에서 발생하는 트랜잭션 당 처리시간으로 통합인증 시스템의 효율성을 확인 하였다.

4.1 보안성 비교분석

통합 인증 시스템의 보안적 안정성을 확인하기 위한 항목은 키의 안전성, Replay Attack 등이 있다. 그리고 기존의 인증시스템과의 비교분석을 위하여 전자여권 표준인 BAC(Basic Access Control), PA(Passive Authentication) 와 웹 서비스 환경의 SSO 인증 시스템에 대한 안정성을 비교 분석 하였으며, 통합 인증 시스템의 보안적 안정성을 분석한 결과는 표2와 같다.

제안하는 통합 인증 시스템은 사용자의 키쌍을 안전하게 교환하는 것을 기반으로 사용자 인증을 수행한다. 사용자의 키쌍을 교환하는 과정에서 생성하는 Serial Number와 Challenge 값을 이용하여 사용자의 공개키를 블록체인 분산 노드에 안전하게 저장하며, 사용자의 개인키는 사용자의 D App 외부로는 전송하는 과정이 없어 유출에 대한 위험성이 없다.

전송되는 사용자의 인증정보는 OTP 모듈이 생성한 랜덤 값을 이용하여 일회성으로 생성하기 때문에 재전송 공격으로부터 안전하며, 불법적인 사용자의 접근을 방지한다. 사용자가 인증을 요청하면, EID Authentication System이 생성한 OTP값과 EID를 조합하여 DAPP에서 QR code 형태로 제공한다.

생성된 QR code는 정해진 시간에 의해 1회만 사용이 가능하며, 서로 다른 인증 과정에 사용하는 인증정보는 매번 변경 된 값이 사용된다. 동일한 EID를 가진 사용자라 하더라고 인증과정에서 사용하는 인증 정보의 내용이 변하기 때문에 공격자가 중간에 메시지를 가로채어 재전송 공격에 사용 할 수 없다.

사용자에게 EID를 발급하고, 인증 정보를 이용한 인증 과정은 웹 환경을 기반으로 동작 된다. 통합인증 시스템에서 전송되는 데이터는 사용자 DAPP과 운영주체 시스템이 교환한 키쌍으로 암호화 및 전자서명 처리 후 분할 한 형태로 전송된다. 또한 사용자와 Verifier(OSP)가 참여하는 EID Authentication을 구성하는 블록체인 네트워크는 안전한 채널을 형성하는 것을 전제로 하여 Packet Sniffing에 대해 안전성을 확보 할 수 있다.

Table 2. Safety Comparison

	BAC	PA	SSO	Proposal
Key safety	-	-	safety	Safety
Replay Attack	safety	safety	-	Safety
Packet Sniffing	safety	safety	safety	Safety

4.2 효율성 비교분석

제안하는 통합인증 시스템의 효율성을 성능 분석하기 위해, 스마트카드 기반의 사용자 인증 시스템 A, B사의 트랜잭션의 처리 시간을 비교 분석하였다.

인증과정에서 발생하는 사용자의 App, 발행 및 인증기관의 서버, 서비스 제공기관 서버 사이의 총 처리량을 트랜잭션 당 처리시간으로 비교 분석하였다. 트랜잭션을 1회부터 1000회까지로 구분하여, 각 시스템 별로 처리시간을 측정하였으며, 그 결과는 다음 표3과 같다.

Table 3. Processing time per transaction

	A	B	Proposal
1T	0.613	0.637	0.572
10T	3.474	3.564	3.391
100T	33.892	34.834	33.241
300T	168.291	159.494	153.352
500T	382.454	369.827	336.842
700T	675.244	645.215	613.274
1000T	1321.187	135.274	129.748

5. 결론

본 논문은 블록체인 환경에서 EID를 이용한 사용자 통합 인증 시스템을 제안한다. 제안하는 사용자 통합 인증 시스템은 여러 사이트에서 신원 확인이 가능한 EID를 사용자에게 발급하고, 정보의 거래 간에 발생하는 이력의 위변조 방지와 무결성 검증을 위한 기능을 함께 제공한다.

제안하는 사용자 인증 시스템에서 발급된 EID는 온라인 환경에서 신원정보를 확인하고 검증할 수 있는 신분증 역할을 한다. 기존의 ID는 등록된 사이트만 사용 할 수 있는 것과 달리, EID는 하나의 식별정보로 여러 사이트에서 자신의 신원정보를 제시하고 검증 받을 수 있다. 여러 사이트에 각각의 ID를 등록 할 필요 없는 하나의 통합 ID 기능을 제공한다. EID를 이용한 사용자 인증 시스템은 중앙 집중형 시스템을 탈피하여, 블록체인의 분산 노드에 사용자의 정보를 저장하고 인증 절차에 사용 한다. 기존의 중앙 집중형 시스템이 여러 기관에 대한 인증 시스템을 각각 구축해야 하는 것과 달리 제안하는 사용자 인증 시스템은 사용자가 발급받은 하나의 EID를 통해 여러 기관에서 인증 할 수 있는 시스템을 제공한다.

또한 사용자의 정보를 저장하고, 인증 시스템을 제공하기 위해 사용하는 중앙 집중형 시스템은 해킹 및 개인정보 침해에 대한 위험성을 가지고 있다. 반면 EID를 이용한 통합인증 시스템은 블록체인을 기반으로 하여, 사용자의 인증환경을 보다 안전하게 제공한다.

제안하는 사용자 인증 시스템이 발급 하는 EID는 블록체인 분산 노드에서 사용자의 공개키와 개인키 쌍을 이용하여 신원을 구분하고 검증한다. 사용자가 생성한 키 쌍 중 공개키는 암호화 처리되어 분산 노드에 안전하게 등록되며, 개인키는 Wallet 형태의 DAPP이 설치되어 있는 스마트폰의 보안 영역에서 안전하게 보관된다.

향후 요구하는 사용자 정보 및 보안 수준이 크게 차이가 나는 웹사이트간의 통합인증 적용에 대한 연구와 다양한 Off-line 서비스에 적용 할 수 있는 사용자 인증 시스템의 연구가 추가적으로 필요하다.

References

[1] J. C. Park, "A Secure Single Sign-On Scheme across Multiple Allied Websites using Smartphones". *Journal of Security Engineering*, Vol.14, No.3, pp. 189-204, 2017.
DOI: http://dx.doi.org/10.14257/jse.2017.06.01

[2] Y. Choi , H. Kwon, "A Study on Legal Issues between the Application of Blockchain Technology and Deletion and the Third Party Supply of Personal Information", *Journal of the Korea Institute of Information Security & Cryptology*, Vol.28, No.6, pp.1607-1621, 2018.
DOI: https://doi.org/10.13089/JKIISC.2018.28.6.1607

[3] 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

[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] M. J. Cho, C. H. Lee, "Access Control Mechanism for Industrial Control System Based Smart Contract", *Journal of The Korea Institute of Information Securty & Cryptology*, Vol.29, No.3, pp.579-588, 2019.
DOI: https://doi.org/10.13089/JKIISC.2019.29.3.579

[6] 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

[7] J. K. Lee, J. G. Son, H. M. Kim, H. K. Oh, "An Authentication Scheme for Providing to User Service Transparency in Multicloud Environment", *Journal of The Korea Institute of Information Security & Cryptology*, Vol.23, No.6, pp.1131-1141, Dec 2013.
DOI: https://doi.org/10.13089/JKIISC.2013.23.6.1131

[8] H. Kim, I. Lee, "A Study on Secure and Improved Single Sign-On Authentication System against Replay Attack", *Jr. of the Korea Institute of Information Security & Cryptology*, Vol.24, No.5, pp.769-780, 2014.
DOI: https://doi.org/10.13089/JKIISC.2014.24.5.769

[9] Security Technology Research Team, Comparison of Changes and Characteristics of Identity Information Management Types, Security Research Department, Financial Security Agency, Korea, pp.1-6, 2017.

[10] BSI, Common Criteria Protection Profile-Machine Readable Travel Document with ICAO Application, Extended Access Control with PACE(EAC pp), BSI-PP-0017, Version1.3.0, 20th January 2012.

[11] Gaurav S.,Kcand Paul A.,Karger, Security and privacy issues in machine readable travel documents(MRTDs), IBM Technical Report(RC 23575), IBM T.J, Watson Research Labs, Apr 2005.

[12] BSI, Advanced Security Mechanisms Machine Readable Travel Documents - Extended Access Control(EAC), Version 2.05, TR-03110, 2010.

[13] NIST. "FIPS Publication186-1:Digital Signature Standard(DS-S)", November 2008.

[14] G. W. Kuk, Application Cases by Blockchain Technology and Industry Sectors, Weekly ICT Trends, Institute of Information & Communications Technology Planning & Evaluation, Vol.1900, pp.13-27, 2019.

[15] Y. J. Lee, Taeyeol Jeon.. "An Fingerprint Authentication Model of ERM System using Private Key Escrow Management Server", *Journal of the Korea*

Academia-Industrial, Vol.20, No.6, pp.1-8. 2019.
DOI: https://doi.org/10.5762/KAIS.2019.20.6.1

[16] J. H. Jang, S. H. Song, S. T. Kim, "A Survey on Blockchain Platforms for Supply Chain Management", *The Journal of The Institute of Internet, Broadcasting and Communication*, Vol.18, No.5, pp.259-265, 2019.
DOI: https://doi.org/10.7236/JIIBC.2018.18.5.259

김 재 용(Jai-Yong Kim) [정회원]

- 2010년 2월 : 숭실대학교 일반대학원 컴퓨터공학과 (컴퓨터공학석사)
- 2012년 6월 : 숭실대학교 일반대학원 컴퓨터공학과 (컴퓨터공학박사 수료)

〈관심분야〉
네트워크 보안, 융합 보안

정 용 훈(Yong-Hoon Jung) [정회원]

- 2006년 8월 : 숭실대학교 컴퓨터공학과 (공학석사)
- 2010년 2월 : 숭실대학교 컴퓨터공학과 (공학박사)
- 2011년 3월 ~ 2014년 2월 : 서일대학교 조교수
- 2018년 8월 ~ 현재 : 바스랩 연구소장
- 현) 한국산학기술학회 상임이사

〈관심분야〉
네트워크 보안, 융합 보안

전 문 석(Mon-Seog Jun) [정회원]

- 1989년 2월 : University of Maryland Comuter Science (공학박사)
- 1989년 3월 ~ 1991년 2월 : New Mexico State University Physical Science Lab. 책임연구원
- 1991년 3월 ~ 현재 : 숭실대학교컴퓨터학과 정교수

〈관심분야〉
네트워크 보안, 생체 인증

이 상 범(Sang-Be Lee) [정회원]

- 1997년 2월 : 성균관대학교 문헌정보학과 (문헌정보학사)
- 2019년 10월 ~ 현재 : 유니허브랩

〈관심분야〉
네트워크 보안, 융합 보안