사용자 인증 기술 동향과 메타버스에서의 적용 방향 연구

이찬희[1], 아비르[1], 강정호[2], 박지수[3], 박종혁[1,*]
[1]서울과학기술대학교 컴퓨터공학과
[2]배화여자대학교 컴퓨터아키텍처 데이터베이스설계
[3]전주대학교 컴퓨터공학과
[1]{happilyfly, abir.el, jhpark1}@seoultech.ac.kr
[2]kjh7548@naver.com
[3]jisupark7203@gmail.com

A Study on the Trends of User Authentication Technology and its Future Application in Metaverse

Chan Hee Lee[1], Abir EL Azzaoui[1], Jong Hyuk Park[1,*]
[1]Dept. of Computer Science and Engineering, Seoul National University of Science and Technology

요 약

최근 공인인증서가 폐지되고 보다 발급이 간편하고 유효기간이 긴 사설인증서가 부상했다. 더불어 탈중앙화를 핵심 개념으로 하는 블록체인 기반 분산 신원 증명(Decentralized Identity, DID)기술이 대두되고 있다. 서비스 환경의 변화에 따라 사용자 인증 기술도 변화가 요구된다. 더욱이 메타버스라는 새로운 인터넷 환경이 조성되고 있는 바 현재 사용자 인증 기술의 동향을 살펴보고 미래에 사용자 인증이 나아갈 방향성을 제시하는 것은 의미가 있어 보인다. 본 논문에서는 사용자 인증 기술의 개요와 사용자 인증 기술의 변천과정을 시작으로 공개키 기반 구조(Public Key Infrastructure, PKI)와 분산 신원 증명을 중심으로 시장에서의 사용자 인증 기술의 동향을 살펴본다. 나아가 메타버스가 상용화되었을 시기에 사용자 인증 기술이 나아가야할 세가지 방향성(분산화, 플랫폼 초월, 생체 기반 인증 중심)을 제시한다.

1. 서론

지난 2020년 5월 20일 전자서명법 개정안(공인인증서 폐지법)이 20대 국회 본회의를 통과했다. 이에 따라 21년 동안 사용되었던 공인인증서는 '공인'의 자격을 상실하고 사설인증서의 경쟁력이 제고되었다. 이동 통신 3사(SK텔레콤, KT, LG U+)가 2019년 4월에 내놓은 PASS를 선두로 네이버 인증서와 카카오톡 인증서는 지난 코로나19 팬데믹 시기 질병관리청이 코로나19 백신 사전 예약을 하는 데에 사용자 인증으로 중추적인 역할을 수행했다.

분산원장을 필두로 한 블록체인이 수면 위로 떠오르면서 탈중앙화 신원증명 또한 그 중요성이 증대하고 있다. 신원인증 및 관리 유형이 중앙집중형에서 연합형을 거쳐 분산형으로 바뀌는 것은 변화하는 인터넷 환경과 그 사용자들의 인식 변화를 대변한다.

현 시대의 상황을 살펴 그 다음의 예상되는 변화들에 대해서 사용자 인증기술이 나아가야 하는 방향에 대해 짚어보는 것은 의미가 있어 보인다. 이에 본 논문은 2장에서 사용자 인증기술의 개요와 대한민국의 사용자 인증기술의 변천 과정을 조명한다. 3장에서 현재 사용되고 있는 사용자 인증기술의 동향을 살펴본다. 4장에서 메타버스로 대표되는 미래에 필요한 사용자 인증 기술의 접근 방향을 제시하고 마지막 5장에서는 결론에 도달한다.

2. 사용자 인증기술의 개요와 변천과정

사용자 인증기술에 대해 간략히 살펴보고 주민등록번호, 전자서명, 아이핀, 공인인증서 순서로 사용자 인증 기술의 변천과정을 조명한다.

2.1 사용자 인증기술의 개요

인증은 메시지의 무결성을 검증하는 메시지 인증과 정당한 사용자의 접속인지를 확인하는 사용자 인증으로 크게 구분할 수 있다.

사용자 인증(User Authentication)의 유형에는 지식, 소유, 존재, 행위가 있으며 각각의 대표적인 예시로는 패스워드, 신분증, 홍채, 걸음걸이 등이 있다[1].

2.2 사용자 인증기술의 변천과정

주민등록법은 1962년 법률 제1067호로 제정된 후 30여 차례의 개정을 거쳐 오늘날에 이른다. 행정 효율성 제고를 목적으로 한 주민등록제도가 정보사회의 발전에 따라 인터넷상의 본인 신원확인의 수단이 되는 것에는 그리 오랜 시간이 걸리지 않았다. 다만, 프라이버시의 개념이 비대해짐에 따라 주민등록 번호의 오남용은 큰 사회문제로 대두된 바, 정부는 새로운 신원확인 수단이 필요했다[2].

1990년대 후반 초고속정보통신기반의 구축으로 민간부문에서는 전자상거래가 급속하게 확산되었다. 신원증명을 위한 새로운 수단이 요구되었고, 그 해결책으로 '전자서명'이 등장한다. 그 핵심은 공인인증기관이 확인한 전자 서명을 서면 상의 기명날인과 동일한 법적 효력을 부여하는 것으로 본격적으로 공인인증서가 전자상거래에서 신원확인의 수단으로 활용되기 시작한다[3].

공인인증서와 더불어 2006년 10월 정보통신부는 '인터넷상의 주민번호 대체수단 가이드라인'을 정하고 가상주민번호, 개인인증키, 개인ID인증 등 여러 명칭으로 불리는 대체수단의 명칭을 '아이핀(i-PIN)'으로 통합했다. 그러나 실정법에 의해 이를 강제하지 않고 사용을 권장하는 수준에 그쳐 활성화되지는 못했다[4].

전자서명법에 근거한 공인인증서는 지난 20년 동안 인터넷뱅킹, 온라인증권을 비롯한 다양한 분야에 활발하게 사용되어 왔으나 의외의 곳에서 문제가 터진다. 인터넷익스플로러를 위한 플러그인(plug-in)인 'ActiveX'를 통해 개인정보 유출이나 해킹사고가 빈번히 발생하는 것이다. 이에 공인인증서 사용 시 필수 설치가 요구되는 'ActiveX'를 제거하기 위한 정책이 추진된다. 2014년 10월 1일 전자금융거래법 개정안이 통과되며 공인인증서의 의무조항이 삭제되고 2018년에 공인인증서는 본격적인 폐지 수순을 밟았다. 2020년 5월 20일 마침내 20년 만에 공인인증서 폐지를 골자로 하는 전자서명법 개정안이 의결되었고, 추가로 국무회의 의결을 통해 6월 9일 공표되면서 2020년 12월 10일을 기점으로 공인인증서는 사라지게 되었다[5].

PASS, 네이버, 카카오페이 등의 민간인증서들이 간편한 발급과 폭 넓은 사용으로 공인인증서의 자리를 빠르게 메꾸고 있으며 분산 신원 증명 기술이 탈중앙화를 앞세워 부상하고 있다[6]. 3장에서는 사용자 인증기술의 동향을 살펴본다.

3. 사용자 인증기술의 동향

PASS, 네이버 인증서, 카카오페이 인증서로 대표되는 사설인증서는 공인인증서와 기술적인 차이점은 없다. 공개키 기반 구조를 사용하기 때문이다[7]. PKI는 신뢰할 수 있는 인증 기관(Certificate Authority, CA)에서 부여된 한쌍의 공개키와 개인키를 사용함으로써 안전한 데이터 교환이 가능하게 한다. 다만 사설인증서가 공인인증서보다 간편한 이유는 기존의 공인인증서가 암호화된 파일을 사용자가 자신의 PC하드나 이동식 디스크에 보관하도록 했다면 사설인증서는 해당 기업에서 관리하기 때문이다. 사용자 입장에서는 인증서 파일을 관리, 보관할 필요가 없어짐과 동시에 직접 해킹 위험을 막아내지 않아도 되니 보안 프로그램 또한 설치하지 않아도 되는 것이다. 현재 PKI 기반 사설인증서에는 앞선 3개 말고도 뱅크샐러드, 페이코, 토스, 삼성패스 등이 있다.

PKI를 비롯한 기존 대부분의 신원확인 서비스는 중앙화된 시스템에 의해 통제, 관리된다. 하지만 이러한 방법은 서비스 제공 기업, 혹은 최상위 인증기관에게 사용자의 신원정보가 집중되며 중앙기관의 보안이 취약해지면 수많은 개인정보 유출과 프라이버시의 침해가 예상된다는 문제점이 있다. 이에 대비하여 2018년 암호화폐를 등에 업고 등장한 블록체인 기반의 탈중앙화 신원증명는 분산된 시스템을 통해 특정 기업에 대한 종속없이, 사용자가 자신의 정보를 관리하고 서비스 제공 기업에게 필요한 정보만을 선택적으로 제공할 수 있다는 장점이 있다. DID 얼라이언스, 마이키핀얼라이언스, 마이아이디얼라이언스, 이니셜DID연합 등이 분산신원증명 기술을 개발하고 있고, 부산블록체인 특구 사업으로 모바일 신원 인증 서비스 B PASS가 진행중에 있다. 한편 카카오와 네이버는 DID 기술을 자사의 모델에 접목중에 있다.

당분간 신원 인증 시장에서 공개키 기반 구조와 분산신원증명의 치열한 경쟁이 예상되지만 블록체인을 기반으로 하는 분산신원증명의 강세가 점차 이어질 것으로 보인다.

4. 메타버스에서 사용자 인증기술의 접근 방향

메타버스(metaverse)란 초월(meta)과 우주(universe)의 합성어로 현실을 디지털 기반의 가상세계로 확장해서 다루는 개념이다[8]. 이러한 메타버스에서는 가상의 '나' 또는 '디지털 미(Digital Me)'

가 현실의 '나'를 대체하는 데 이를 '아바타(Avatar)'라고 한다.

메타버스가 상용화가 된다면 아바타의 본인인증 방식은 지금의 본인인증 방식과는 달라야 한다. 특히 아바타 보안의 경우 정당하지 않은 자가 타인 행세를 할 경우 메타버스 자체가 또 하나의 현실을 표방하는 바 금융과 물품 거래를 포함하여 그 피해는 적지 않을 것으로 예상된다. 세가지 측면에서 살펴보면, 메타버스 속 사용자 인증은 첫째로 분산화 되어야 한다. 둘째로 플랫폼을 초월해야한다. 셋째로 생체 인증 중심이 되어야 한다. 하나씩 살펴보겠다.

먼저, 현재에 대두되고 있는 탈중앙화 신원인증은 메타버스가 상용화된다고 해서 상장되어야 할 기술이 아니다. 중앙집중형 모델은 인증 서비스 구축 및 이용이 편리하다는 장점이 있지만 해킹 및 프라이버시 침해와 같은 문제가 계속해서 제기되는 바 분산화된 신원인증은 메타버스 속 사용자 인증에서도 유용한 기술이 될 것이다.

다음으로, 메타버스 서비스는 스마트폰과는 또 다른 단말기를 통해 접속하여 진행되는 것들이 많을 것이며 그 시스템은 빅데이터, 클라우드, 네트워크 등이 융합된 구조로 복잡한 양상을 띌 전망이다. 단말기와 시스템의 종류별로 인증기술이 상이하게 된다면 메타버스 속에서 이루어지는 거래는 상호 인증 과정에서 충돌이 일어날 것이다. 따라서 플랫폼을 초월한 공통된 형식을 가질 필요가 있다.

끝으로, 메타버스에서 사용자가 아바타를 움직이기 위해서는 자신의 신체를 이용해야 한다. 이것은 '뇌-컴퓨터 인터페이스(Brain-Computer Interface)' 기술의 발전으로 인해 뇌파만으로 아바타를 조종한다고 해도 마찬가지이다[9]. 그에 반해 지식기반 인증과 소유기반 인증은 잊어버릴 가능성과 분실의 위험으로 그 활용도와 편의성에서 생체기반 인증에 비해 부족한 것은 사실이다. 따라서 메타버스에서의 사용자 인증은 생체기반 인증을 중심으로 구성할 필요가 있어 보인다.

5. 결론

본 논문 사용자 인증기술의 개요를 간략하게 살펴보고 1962년에 제정된 주민등록법을 시작으로 사용자 인증기술의 변천과정을 짚어보았으며 공인인증서의 폐지로 대두된 사설인증서와 탈중앙화를 핵심 개념으로 하는 분산인증증명을 통해 사용자 인증기술의 동향을 살펴보고 미래에 메타버스가 상용화 되었을 시기에 대한 사용자 인증 기술의 접근에 대해 세 가지 방향성(분산화, 플랫폼 초월, 생체 기반 인증 중심)을 제시했다. 본 논문에서는 사용자 인증에 집중해 보안의 측면을 집중했지만 향후 연구에서는 프라이버시의 측면에서 메타버스가 상용화되면 발생할 사생활 이슈에 대한 연구를 진행하고자 한다.

Acknowledgement

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2022R1F1A1071926)

참고문헌

[1] 최은정, 김찬오, 송주석, "공개키 암호 기법을 이용한 패스워드 기반의 원거리 사용자 인증 프로토콜", 정보과학회논문지: 정보통신 제 30권, 제 1호, 2쪽, 2003

[2] 고문현, "주민등록제도의 문제점과 개선방안", 공법학연구, 제 13권, 제 4호, 269-293쪽, 2012

[3] 김영준, "전자서명과 인증에 관한 연구", 통상정보연구, 제 3권, 제 1호, 83-104쪽, 2001

[4] 장인용, 염흥열, "인터넷상의 본인확인수단인 아이핀의 활성화 방안 연구", 정보보호 학회지, 제 19권, 제 5호, 81-94쪽, 2009

[5] 진승헌, 조진만, 김수형, "공인인증서 20년의 주요 이슈와 시사점", 한국정보기술학회 추계 종합학술대회 논문집, 한국, 2021, 16-20쪽, 2021

[6] 전재영, 우 사이먼, "신분증을 이용한 블록체인 기반의 분산원장 인증 시스템", 2021 한국정보기술학회 추계 종합학술대회 논문집, 한국, 2021, 655-660쪽

[7] 김지연, 박성준, "공개키 기반구조에 관한 고찰", 정보보호학회지, 제 7권, 제 2호, 55-72쪽, 1997

[8] 양경란, 윤성철, 박수경, 이봉규, "디지털트윈 기반의 인더스트리 메타버스: 사례분석을 통한 프레임워크의 정립", 멀티미디어학회논문지, 제 25권, 제 8호, 1122-1135쪽, 2022

[9] 전황수, "뇌-컴퓨터 인터페이스(BCI) 기술 및 개발 동향", 전자통신동향분석, 통권, 131호, 123-133쪽, 2011