AI 기반 다중요소인증 기술을 활용한 패스워드리스 인증시스템 정책적 도입 전략

정다은, 윤수연*
국민대학교, *국민대학교

jde3424@kookmin.ac.kr, *1104py@kookmin.ac.kr

A Policy Adoption Strategy for Passwordless Authentication Systems Using AI-Based Multi-Factor Authentication(MFA)

Jeong Da Eun, Soo-Yeon Yoon*
Kookmin Univ., *Kookmin Univ.

요 약

전통적인 비밀번호 인증 방식이 갖는 고질적인 보안 취약 문제를 해소하기 위해 패스워드리스 인증 시스템이 대두되고 있다. 이는 사용자 단말기에서 직접 키를 생성 및 저장하여 인증하기 때문에 중앙 서버에 저장된 인증 정보나 개인정보의 유출로 말미암아 발생할 수 있는 각종 보안 위협을 예방하는데 효과적일 것으로 기대한다. 또한 단일 인증만으로는 안전한 사이버 환경을 보장할 수 없기에 다중요소인증 기술의 활용은 필수적이다. 더불어 “신뢰하지 말고 항상 검증하라(Never Trust, Always Verify)”라는 제로 트러스트(Zero Trust) 보안 모델의 핵심 원칙에 따라 AI 기술과 사용자 고유의 특징을 활용한 다각적, 지속적 인증이 가능하도록 함으로써 로그인 이후 발생하는 공격을 차단할 수 있다. 이러한 차세대 인증시스템을 위한 선제적 접근을 통해 최근 연이어 발생하는 개인정보 유출 사고와 계정 탈취로 인한 2 차 금융사기 등 심각한 범죄로의 확산을 예방하고 디지털 안전사회를 구축하기 위한 정책적 전략을 제시하고자 한다.

Ⅰ. 서론

온라인 서비스 이용이 증가함에 따라 다수의 비밀번호를 관리해야 하는 문제에 봉착하면서 비밀번호 재사용이 빈번하게 발생하고 있으며 이를 악용한 크리덴셜 스터핑(Credential Stuffing)이 사회적 문제로 대두되고 있다. 이는 유출된 비밀번호를 다른 사이트에서 로그인에 성공할 때까지 입력하는 공격 방식으로 동일한 비밀번호를 다수의 사이트에서 중복 사용하는 사용자의 피해가 커질 수밖에 없다. 2023 년 국내에서는 인터파크, 지마켓, 스타벅스 등에서 해당 공격으로 인해 상품권 및 충전금 도용 등의 금전적 피해가 발생된 바 있다. 대응 방안으로 다중요소인증(Multi-Factor Authentication, MFA) 등 추가 보안 수단이 도입되고 있지만 다양한 사이버 공격의 증가로 인해 중앙 서버에 저장된 정보로 사용자를 인증하는 기존 환경에서는 앞서 서술한 근본적인 문제를 해결하기에는 역부족이다. [1] [2]

2025 년 4 월 발생한 SKT 유심 정보 유출 사건 또한 가입자 정보를 관리하는 중앙 서버의 악성코드 감염으로 발생했다. 사용자의 직접적인 인증 정보가 유출된 사고는 아니지만 연일 보안 위협을 우려하는 자극적인 보도가 더해져 국민적 불안감을 증폭시켰다. 빠져나간 유심 정보를 활용하여 불법 복제폰이 만들어질 경우 부정 금융거래로 이어질 수 있다는 우려가 커졌기 때문이다. 이와 관련하여 금융감독원은 금융사에 공문을 보내 “휴대전화 본인인증, SMS 인증만으로 인증이 완료되는 경우에는 추가 인증수단을 고려하라”고 당부하는 등 금융계를 중심으로 추가적인 범죄 확산을 막기 위한 긴급 예방 조치에 나섰다.

반면, 최근에 대두된 패스워드리스 인증(Passwordless Authentication)은 사용자 단말기에서 직접 생성한 키와 생체정보를 활용하여 비밀번호 없이 사용자를 인증하고 서비스에 접근할 수 있도록 하는 인증 방식을 의미한다. 사용자가 비밀번호를 기억하지 않아도 되는 편의성이 크다는 점과 중앙 서버가 아닌 사용자 단말기에 키가 저장되는 분산형 구조라는 점에서 차세대 인증시스템으로서 살펴볼 가치가 충분하다. [3]

본 논문에서는 보다 안전한 패스워드리스 인증 시스템 도입을 위하여 AI 기반 다중요소인증 기술 활용 방안을 중심으로 정책적 전략을 제안하고자 한다.

Ⅱ. 이론적 고찰

2.1 패스워드리스 인증시스템 개요

패스워드리스 인증 방식은 생체 정보, 행동, 비대칭키, 물리적 토큰, 보안키 등을 활용하여 인증이 이뤄지기 때문에 텍스트 기반 비밀번호에 의존하지 않는 인증 매커니즘을 가지고 있다. [2] 패스워드리스 인증 방식의 가장 대표적인 예는 패스키(Passkey)이다. 패스키는 FIDO2 표준 기반의 인증 방식으로 사용자 기기에서 공개키-개인키 쌍을 생성하여 개인키는 해당 단말기 내에 보관하고, 공개키는 해당 애플리케이션 서버에 보관한다. 로그인 요청 시 사용자의 기기가 개인키로 로그인 요청을 암호화하여 서버로 전송하고 이를 수신한 서버는 가지고 있는 공개키로 검증하기 때문에 이 과정에서 비밀번호를 애플리케이션 서버 단에 저장해두지 않아도 된다. 대표적으로 Apple 사의 Face ID,

Touch ID, iCloud Keychain, Google 의 패스키 로그인, Microsoft 의 Windows Hello 등이 이에 해당한다.

이러한 패스워드리스 인증 방식에도 한계점은 존재하는데, 인증 앱, 푸시 알람, 모바일 단말기 사용으로 인해 해당 인증 수단에서 장애가 발생하는 경우 정상 권한자의 접근제한이 발생할 수 있다. 또한, Eric Klieme et al.(2020)는 성공적인 로그인 이후에 사용자를 지속적으로 인증하지 않아 공격자를 탐지할 수 없다는 문제를 지적했다. [4]

2.2 AI 기반 다중요소인증 기술 개요

2.2.1 다중요소인증 기술 개념

다중요소인증은 최소 두 가지 이상의 인증 요소를 이용하여 본인 여부를 인증하는 것을 의미한다. 사용자가 알고 있는 요소(지식 요소), 사용자가 소유하고 있는 요소(소유 요소), 사용자만의 고유 요소(신체속성 요소) 등에서 최소 2 개 이상을 함께 사용하여 인증한다. 일반적으로 기존의 아이디와 비밀번호 외에 이메일 인증, SMS 인증, 음성 통화 인증, OTP 등을 함께 활용한다. [5]

Hassan 과 Shukur(2021)는 비밀번호, 생체인식, OTP 를 결합하여 다중요소인증 기반 사용자 인증시스템의 보안을 향상시키는 프레임워크를 제시했지만, 여전히 심 스와핑 공격, SMS 인증 중간 탈취, 악성코드 등에 취약한 한계가 존재한다. [6]

2.2.2 AI 기술 적용의 필요성

AI 기술을 통해 사용자만의 고유한 행동적 특징을 학습하여 신원을 다각적으로 검증하고 동시에 사용자의 중간 개입 없이 지속적으로 인증함으로써 로그인 이후 발생할 수 있는 공격을 효과적으로 차단할 수 있다. 사용자의 얼굴, 음성, 보행, 로그인 패턴, 접속 위치 등의 데이터를 종합적으로 분석하여 기준 프로파일(Profile)을 설정해두고 최초 로그인 이후 시간 경과에 따른 사용자 활동 모니터링 및 이상패턴 식별이 가능하다. [7]

2.2.3 AI 기술을 활용한 사용자 인증에 관한 선행 연구

Upal Mahbub et al.(2019)는 모바일 환경에서 가려지거나 부분적으로 보이는 얼굴(Partial Face)만으로도 인증이 가능한 얼굴 검출 기술을 제시하였고, Daniel Garabato et al.(2022)는 AI 기술을 활용한 마우스 움직임 분석을 통해 사용자 행위 기반 연속 인증 시스템을 제안했다. [8] [9]

Yun Da Hye(2025)는 사용자가 암호화해둔 키워드를 활용하여 인증 시도마다 생성형 AI 를 통해 새롭게 생성된 이미지를 선택하도록 함으로써 별도의 인증 기기를 사용하지 않는 생성형 AI 를 활용한 이미지 기반 다중 인증 기법을 제시하였다. [10]

Ⅲ. 결론 및 정책적 제언

본 연구는 날로 정교해지는 사이버 위협 환경 속에서 패스워드리스 인증시스템의 실효성을 확보하기 위한 방안으로서 AI 기반 다중요소인증 기술의 적용 가능성과 전략에 대해 다각적으로 분석하였다. 특히, [그림 1]과 같이 단기-중기-장기적 발전 단계에 따라 정책적 도입 전략을 구체화하였다.

단기적으로는, 즉시 적용 가능한 AI 사용자 인증 기술의 가이드라인을 제시하고, 활용 가능한 환경 조성 및 대국민 소통 체계 마련, 관련 제도의 정비가 필요함을 확인하였다. 이는 초기 기반 조성과 국민 수용성 확보를 위한 핵심 단계로, AI 인증 기술의 신뢰도를 제고하는 중요한 출발점이 된다.

중기적으로는, 정부 주도의 R&D 및 공공 우선 도입을 통해 기술의 고도화 및 제도적 뒷받침이 필수적이다. 특히, AI 인증 시스템의 적용 확산을 위해 실증사업 추진, 민간 산업기반 강화, 데이터 협업 체계 구축, AI 보안 인력 양성 등이 병행되어야 한다. 이를 통해 기술의 성능 검증과 사회적 신뢰 확보가 가능해질 것이다.

장기적으로는, AI 기반 패스워드리스 인증시스템의 국제 표준화 추진과 함께 지속가능한 인증 생태계를 구축해야 한다. 이 과정에서 국내 인증 표준 마련, AI 인증 운영의 안정성 확보, 관련 법령·규제 정비가 동반되어야 하며, 이는 국내외 시장에서의 기술 경쟁력을 확보하는 데 핵심적 요소로 작용할 수 있을 것이다.

그림 1. AI 기반 다중요소인증 기술을 활용한 패스워드리스 인증시스템 정책적 도입 전략

이처럼 체계적인 전략을 통해, AI 기반 다중요소인증 기술은 Gen BI 로 더 확장되어 향후 패스워드 기반 인증을 대체할 수 있는 신뢰성 높은 미래 인증수단으로 자리 잡을 수 있을 것이다. 본 연구는 현실적 정책 수립 및 인증시스템 설계에 있어 실질적 근거 자료로 활용될 수 있으며, 접근성 및 신뢰성이 강화된 보안서비스 도입의 방향성 제시에 기여할 것으로 기대된다.

참고 문헌

[1] Al-Ameri, Hanan Hussein, and Serkan Ayvaz, "A blockchain-based secure mutual authentication system for E-government services," *2023 3rd International Scientific Conference of Engineering Sciences (ISCES)*, pp. 19-24, 2023.

[2] Yusop, Mohd Imran Md, et al, "Advancing Passwordless Authentication: A Systematic Review of Methods, Challenges, and Future Directions for Secure User Identity," *IEEE Access*, pp. 13919-13943, 2025.

[3] Laborde, Romain, et al, "A user-centric identity management framework based on the W3C verifiable credentials and the FIDO universal authentication framework," *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf. (CCNC)*, pp. 1-8, 2020.

[4] Klieme, Eric, et al, "FIDOnuous: A FIDO2/WebAuthn extension to support continuous Web authentication," *Proc. IEEE 19th Int. Conf. Trust Secur. Privacy Comput. Commun. (TrustCom)*, pp. 1857-1867, 2020.

[5] AWS, "다중 인증(MFA)이란 무엇인가요?," [온라인]. Available: https://aws.amazon.com/.

[6] Ali, Guma, Mussa Ally Dida, and Anael Elikana Sam, "A secure and efficient multi-factor authentication algorithm for mobile money applications," *Future Internet*, 제 13, 번호: 12, p. 299, 2021.

[7] 김수형, "AI 를 이용한 사용자 인증 기술 동향," 정보과학회, 2021.

[8] Mahbub, Upal, Sayantan Sarkar, and Rama Chellappa, "Partial face detection in the mobile domain," *Image and Vision*, 제 82, pp. 1-17, 2019.

[9] Garabato, Daniel, et al, "AI-based user authentication reinforcement by continuous extraction of behavioral interaction features," *Springer*, 제 34, 번호: 14, pp. 11691-11705, 2022.

[10] 윤다혜 그리고 한요섭, "생성형 AI 를 활용한 이미지 인증 기반 다중 인증 기법에 관한 연구," %1 *한국통신학회 동계종합학술발표회*, 2025.