분산 식별자 메소드 별 보안 취약점 분석

장현지*, 김건민**, 김경백***

요 약

기존의 중앙 집중식 신원 관리는 상호운용성과 사용자의 편의성을 보장하였으나, 중앙 집중형 ID 제공자에 대한 과도한 의존이라는 구조적 한계로 인해 단일 실패 지점, 대규모 침해 사고 등의 보안 취약점을 노출했다. 이를 극복하기 위해 등장한 탈중앙화 식별자(Decentralized Identifier, DID)는 사용자 중심의 신원 관리를 가능하게 하며 자기 주권 신원(Self-Soverign Identity, SSI)의 핵심 기술로 부상하였다. DID는 다양한 기술적 기반 위에서 구현되며, 이에 각 DID Method는 상이한 보안 취약점을 내포한다. 이 논문은 5가지 DID Method에 대한 보안 취약점을 체계적으로 분석하고, 이를 바탕으로 사용 맥락에 적합한 DID Method 선택 방안을 제시한다.

Ⅰ. 서 론

디지털 시대의 발전과 함께 온라인 환경에서의 신원(Identity)의 확인 및 관리의 문제는 기술적으로 핵심 의제가 되어왔다. 초기의 중앙 집중형 신원 관리 체계인 OAuth2.0과 OpenID [1] 등은 상호운용성과 편의성을 제공했으나, 이는 중앙 집중형 ID 제공자(Identity Provider, IdP)에 대한 과도한 의존으로, 데이터 중앙 집중이라는 구조적 한계를 노출했다.

이에 World Wide Web Consortium(W3C)는 블록체인 및 분산 원장 기술(Distributed Ledger Technology, DLT)을 활용한 탈중앙화 신원관리 체계인 DID를 제안하였다 [2]. DID는 SSI의 [3] 기반 기술로 자리 잡았으며, 유럽의 EBSI [4], 한국의 K-BTF 등 국가 단위의 신원 시스템 도입이 진행되고 있다. 특히 DID는 단일한 기술 스택에 국한되지 않고, 다양한 구현 방식(Method)을 통해 발행될 수 있다는 특징을 지닌다. W3C DID Method Registry에는 백여개 이상의 DID Method [5-6] 가 등록되어 있으며, 이는 웹 인프라, 순수 암호학, 퍼블릭 블록체인 등 다양한 기술적 기반을 포괄한다 [7-9]. DID Method의 다양성은 각 Method 별로 상이한 보안 취약점을 의미하나, 이에 대한 연구는 미비하다. 이에 본 연구는 대표적인 다섯 가지 DID Method(did:web, did:key, did:ethr, did:ion, did:indy)의 보안 취약점을 분석하고, 사용 맥락에 따른 선택 가이드라인을 제시한다.

Ⅱ. DID Method 별 보안 취약점 분석

2.1. did:web 보안 취약점

did:web은 기존 웹 인프라를 활용하여 구현의 단순성과 접근성의 강점을 보이나, 동시에 전통적인 웹 보안 취약점을 그대로 계승한다. DNS 공격은 가장 대표적 위험으로, DNS 캐시 포이즈닝이나 스푸핑을 통해 사용자가 악의적인 서버에서 위조된 DID 문서를 받도록 유도할 수 있다. 또한, 도메인 하이재킹은 더욱

본 연구는 한국인터넷진흥원(KISA)-정보보안 특성화대학 지원사업의 지원을 받아 수행된 연구임(50%). 이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-지역지능화혁신인재양성사업의 지원을 받아 수행된 연구임(IITP-2025-RS-2022-00156287, 50%).

* 전남대학교 AI융합대학 인공지능학부 (학부생, gka1225@jnu.ac.kr)
** 전남대학교 일반대학원 인공지능융합학과 (대학원생, geonminkim@jnu.ac.kr)
*** 교신저자(corresponding author) : 전남대학교 일반대학원 인공지능융합학과 (교수, kyungbaekkim@jnu.ac.kr)

치명적인 위협으로, 도메인 등록 만료나 관리자 계정 침해를 통해 공격자가 도메인 전체를 장악하면 해당 도메인의 DID가 완전히 통제될 위험이 있다. DID 문서를 제공하는 웹 서버 자체의 보안 수준도 중요한 변수로, 애플리케이션 취약점이나 잘못된 설정은 DID 문서의 조작을 허용할 수 있다. 즉, did:web은 편리한 초기 도입에 적합하나, 장기적이고 고보안 환경에서는 위험이 크다.

2.2. did:key 보안 취약점

did:key는 외부 인프라에 의존하지 않는 순수 암호학적 접근으로, 네트워크 기반 공격에는 상대적으로 안전하다. 그러나, 개인키 침해시 복구 불가능성이 가장 큰 문제로 지적된다. 개인키가 분실되거나 탈취되면 DID 자체가 영구적으로 사용 불가능해지며, 기존 신원 연속성이 단절된다. 키 회전 불가능성도 장기적 보안의 치명적인 제약이다. 보안적인 측면에서는 정기적 키 교체가 권장되는 것이 일반적이나, did:key에서는 키 변경은 곧 새로운 DID의 발급을 의미하여 이는 기존의 모든 관계와 인증 정보의 단절을 초래한다.

2.3. did:ethr 보안 취약점

did:ethr는 이더리움 블록체인을 기반으로, 블록체인의 불변성과 투명성을 보안 자산으로 활용한다. 그러나 이 방식에는 스마트 컨트랙트의 취약성이 존재한다. 컨트랙트 코드에 버그나 권한 관리 오류가 있으면 공격자가 DID를 탈취하거나 임의 변경할 수 있다. 둘째, 가스비와 네트워크 혼잡 문제가 DID 운영을 방해할 수 있다. 공격자가 네트워크를 혼잡하게 만들어 거래 수수료를 급등시키면, 정상 사용자가 DID를 갱신하거나 키를 교체하는 것이 사실상 불가능해진다. 이는 Denial of Service(DoS) 공격에 해당한다.

2.4. did:ion 보안 취약점

did:ion은 Sidetree 프로토콜을 기반으로 비트코인 블록체인과 분산 파일 시스템(IPFS)을 결합한다. 이를 통해 대규모 DID 발행과 관리가 가능하며, 고확장성을 보장한다. 그러나, 이러한 하이브리드 구조는 새로운 보안 위협을 수반한다. 첫째, 오프체인 데이터 무결성이다. DID 상태 변경의 대부분이 IPFS와 같은 오프체인 저장소에 기록되므로, 데이터 유실이나 불일치가 발생할 경우 DID 해석이 불안정해진다. 둘째, 앵커링 지연과 검증 문제도 존재한다. 모든 변경 내역은 최종적으로 비트코인 블록체인에 앵커링되나, 블록 생성 시간과 네트워크 혼잡으로 인해 변경 반영이 지연될 수 있으며, 이는 긴급 상황에서의 키 교체와 같은 보안 대응에 취약성을 초래할 수 있다.

2.5. did:indy 보안 취약점

did:indy는 Sovrin 네트워크를 기반으로 하는 허가형 블록체인 DID이다. 퍼블릭 블록체인에 비해 운영 주체가 제한적이므로, 효율적이고 예측 가능한 거버넌스를 제공한다. 그러나 허가형 구조는 동시에 운영자 신뢰성 문제를 수반한다. 합의 알고리즘을 운영하는 검증 노드가 제한적이므로, 특정 운영자의 악의적 행위나 보안 침해는 DID 전체의 신뢰성에 위협이 된다. 합의 프로토콜의 보안성 또한 중요한 변수이다. Indy는 BFT(Byzantine Fault Tolerance)계열의 합의를 사용하나, 참여 노드 수가 제한적일 경우 특정 노드 집단에 의한 담합 가능성이 존재한다.

Ⅲ. 사용 맥락별 DID Method 선택 전략

각 DID Method는 고유한 장점과 취약점을 동시에 지니며, 절대적으로 안전하거나 우월한 방식은 존재하지 않는다. 따라서, DID 도입자는 자신의 사용 맥락과 보안 요구 수준에 따라 가장 적절한 Method를 선택하여야 한다. 본 장에서는 다양한 활용 맥락 별 DID Method 선택 가이드라인을 제시한다.

금융 환경에서는 불변성과 감사 가능성이 핵심적이다. 거래 기록의 위변조가 방지되고, DID 상태 변경 이력 추적이 가능해야한다. 이에 did:ethr의 퍼블릭 블록체인의 투명성과 보안성을 직접 활용할 수 있으며 did:ion의 대규모 확장성과 함께 비트코인 플록체인 앵커링을 통한 무결성 보장을 활용할 수 있다.

의료 환경에서는 데이터 기밀성과 환자 정보 보호가 우선시된다. 또한, 개인 키 관리가 분산되어야 하며, 동시에 장기적인 신원 연속성이 보장되어야 한다. 이

경우 허가형 블록체인을 기반으로 하여 참여 노드가 제한되어 환자 정보의 무단 노출 위험이 낮은 did:indy가 상대적으로 적합하다.

IoT 환경에서는 경량성과 독립성이 중요하다. 센서나 디바이스는 복잡한 블록체인 연산을 처리하기 어렵고, 저전력 기기들이므로 공개키 기반의 did:key가 적합하다. 그러나 키 분실 시 복구가 불가능하다는 한계가 존재하므로, 디바이스 제조 단계에서 안전한 키 보관 장치를 탑재하는 것이 필수적이다.

공공 서비스 환경에서는 상호운용성과 제도적 거버넌스가 중요하다. 다양한 기관이 협력하는 환경에서는 기술적 호환성과 운영 투명성이 확보되어야 하므로, 이 경우 did:web과 did:indy를 혼합하여 did:web을 통해 접근성을 높이고, did:indy의 허가형 합의를 통해 신뢰 기반을 제공할 수 있다.

Ⅳ. 결 론

본 연구에서는 다양한 DID Method는 각기 다른 기술적 기반에 따라 고유한 보안 특성을 지니며, 이에 사용 맥락에 따라 선택의 적절성이 달라진다는 점을 체계적으로 분석하였다. 기존의 DID 관련 연구가 특정 DID Method의 특성이나 DID 자체의 구조적 보안 취약점에 치중하였던 것과 달리, 본 연구는 다섯 가지 대표적인 Method를 구체적으로 비교함으로써 실무적 선택에 실질적 근거를 제공하고자 하였다.

향후 연구에서는 Method별 취약점을 정량적으로 평가할 수 있는 보안 지표의 개발, 실제 공격 시뮬레이션 등 실증적 검증이 필요하다. 이를 통해 DID 생태계의 신뢰성과 안전성 재고에 기여할 수 있을 것이다.

참 고 문 헌

〔1〕 K.Dodanduwa and I. Kaluthanthri, "Role of Trust in OAuth 2.0 and OpenID Connect," 2018 IEEE International Conference on Information and Automation for Sustainability (ICIAfS), Colombo, SriLanka, 2018, pp. 1-4

〔2〕 A. Tabbassum, P. Chintale, C. Akiri and N. Bhasin, "Leveraging Block chain for Secure and Decentralized Identity Management," 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), Pune, India, 2024, pp. 1-6

〔3〕 A. R. Raipurkar, S. Bobde, A. Tripahi and M. Sahu, "Digital Identity System Using Blockchain-based Self Sovereign Identity & Zero Knowledge Proof," 2023 OITS International Conference on Information Technology (OCIT), Raipur, India, 2023, pp. 611-616

〔4〕 TAN, Evrim; DU SEUIL, Daniël. Services Infrastructure (EBSI). *Public Governance and Emerging Technologies: Values, Trust, and Regulatory Compliance*, 2025, 83.

〔5〕 F. Hoops, A. Mühle, F. Matthes and C. Meinel, "A Taxonomy of Decentralized Identifier Methods for Practitioners," 2023 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), Athens, Greece, 2023, pp. 57-65

〔6〕 임도현, 김건민, 조세빈, 진현석, 박태준, 김경백, "Web기반 DID메소드 동향 분석," 2024 한국정보보호학회 호남지부 추계학술대회, 2024

〔7〕 C. Mazzocca, A. Acar, S. Uluagac, R. Montanari, P. Bellavista and M. Conti, "A Survey on Decentralized Identifiers and Verifiable Credentials," in IEEE Communications Surveys & Tutorials

〔8〕 M. -H. Rhie, K. -H. Kim, D. Hwang and K. -H. Kim, "Vulnerability Analysis of DID Document's Updating Process in the Decentralized Identifier Systems," 2021 International Conference on Information Networking (ICOIN), Jeju Island, Korea (South), 2021,pp. 517-520

〔9〕 B. G. Kim, Y. -S. Cho, S. -H. Kim, H. Kim and S. S. Woo, "A Security Analysis of Blockchain-Based Did Services," in IEEE Access, vol. 9, pp. 22894-22913, 2021