https://doi.org/10.33778/kcsa.2023.23.4.017

DID 기술에 기반 한 분산 신원 인증 시스템

시 정*, 신 승 수**, 한 성 화***

요 약

전통적인 인증 시스템은 중앙 집중식 신원 관리 시스템에서 일반적으로 사용자 이름과 비밀번호를 입력하는 방식으로 인증한다. 이러한 인증 방식의 불편함을 개선하기 위해, 분산신원기술을 사용하여 탈중앙화신원증명(DID : Decentralized Identifier)에 기반 한 분산신원인증 시스템을 제안한다. 제안한 시스템은 QR 코드 스캔 방식으로 로그인하는 방식으로 분산신원인증 시스템이다. 블록체인 기술을 사용함으로써 사용자 신원의 고유성과 안전성을 보장할 수 있어 로그인 과정에서 보안성이 향상된다. 제안한 시스템은 DID를 사용하고 InterPlanetary File System(IPFS)를 통합하여 조직 구성원의 신원 정보를 안전하게 비공개로 관리한다. 본 연구에서 제안하는 분산 신원 인증 시스템을 사용하면, 조직 구성원의 보안 및 개인 신원 관리를 효과적으로 수행할 수 있다. 본 연구에서 제안하는 시스템을 활용하기 위해 솔루션으로 확장하기 위한 연구가 필요하다.

Distributed Identity Authentication System based on DID Technology

Chai Ting*, Seung-Soon Shin**, Sung-Hwa Han***

ABSTRACT

Traditional authentication systems typically involve users entering their username and password into a centralized identity management system. To address the inconvenience of such authentication methods, a decentralized identity authentication system based on Distributed Identifiers(DID) is proposed, utilizing decentralized identity technology. The proposed system employs QR code scanning for login, enhancing security through the use of blockchain technology to ensure the uniqueness and safety of user identities during the login process. This system utilizes DIDs and integrates the InterPlanetary File System(IPFS) to securely manage organizational members' identity information while keeping it private. Using the distributed identity authentication system proposed in this study, it is possible to effectively manage the security and personal identity of organization members. To improve the usability of the system proposed in this study, research is needed to expand it into a solution.

Key words : Decentralized Identifier, Blockchain, Verifiable Credential, InterPlanetary File System, Identity Authentication

접수일(2023년 09월 06일), 게재확정일(2023년 09월 18일)

* 동명대학교/컴퓨터미디어공학과 (주저자)
** 동명대학교/정보보호학과 (부저자)
*** 동명대학교/정보보호학과 (교신저자)

1. 서 론

전통적인 인증 시스템은 일반적으로 싱글 포인트(Single Point) 신뢰에 의존하므로 싱글 포인트 실패와 민감한 개인 정보에 쉽게 접근할 수 있다. 그리고 다른 시스템 간 상호 운용성이 부족하여 구성원들이 여러 기관에서 자신의 신원을 증명해야 하는 어려움이 있다. 이러한 문제를 해결하기 위해 사람들은 블록체인 기술을 기반으로 한 분산 신원인증 솔루션을 개발하는 데 관심이 증가하고 있다. 블록체인은 분산 신원 식별자(DID : Decentralized Identifier)와 검증 가능한 자격증명(VC : Verifiable Credential)이 보안과 개인 정보 보호의 신원관리에 효과적인 도구이다[1,2].

블록체인을 사용하여 DID 문서와 VC를 저장하고 신원관련 데이터의 보안, 불변성 및 지속성을 보장한다. 인터플래네타리 파일 시스템(IPFS : InterPlanetary File System)은 증명서 및 성적표와 같은 대량의 신원관련 파일을 효율적으로 저장하고 검색하는 데 사용된다[3,4]. 분산 신원인증 및 분산 저장기술을 활용하여, 신원관리 기관을 신원발급 및 권한 있는 검증자로, 사용자를 신원 소지자 및 컨트롤러로, 리소스 응용 계열을 신원 검증자로 사용하여, 신원발급, 제어, 인증 및 공동 유지 메커니즘에서 신원인증 시스템을 구축한다[5].

본 논문에서는 DID를 사용하여 조직 구성원의 고유하고 검증 가능한 식별자를 생성하고 관리할 수 있는 DID 기술에 기반 한 분산신원인증 시스템을 제안한다 .

2. 관련 연구

2.1 신원관리에서 블록체인

신원관리에서 블록체인 기술은 분산되고 안전하고 신뢰할 수 있으며 투명한 신원인증 및 검증 시스템을 구축할 수 있는 큰 잠재력을 제공한다[6,7]. 블록체인 기술은 분산, 변조 불가능 및 지속성의 특성으로 인해 신원관리 분야에서 큰 관심을 받고 있으며, 실제로 uPort, Sovrin 및 Microsoft의 ION 등 블록체인 기반의 신원관리 프로젝트와 솔루션이 많이 있다. 이러한 프로젝트들은 개인과 조직에게 안전하고 프라이버시 보호가 가능하며 사용하기 쉬운 분산 신원관리 도구를 제공하는 데 목표를 두고 있다[8].

2.2 신원 식별자와 검증 가능한 자격증명

DID는 W3C 규격을 따르며, 분산 신원관리 분야의 산업 표준이 되었다. VC은 디지털화된, 신원 관련 정보로서, 학위증명서나 회원 자격과 같은 것들이 포함되며, 발행자가 암호화 서명을 하고 수신자가 검증할 수 있다[9]. 이는 사용자가 자신의 신원 관련 정보를 안전하고 프라이버시 보호를 위한 방식으로 제공할 수 있다. 예를 들어, 사람이 학력을 증명해야 할 때, 관련 없는 개인 정보를 공유하지 않고 검증 가능한 자격 증명을 통해 잠재적인 고용주에게 제공할 수 있다[10].

2.3 조직 구성원의 신원 관리

효과적인 신원관리 시스템은 조직의 데이터 보안, 프라이버시 보호 강화, 업무 프로세스 단순화, 작업 효율성 향상에 기여할 수 있다. 조직 구성원의 신원 관리 시스템을 잘 구현하기 위해, 블록체인 기반의 분산인증시스템을 고려할 수 있다. 이러한 시스템은 분산신원식별자(DID) 및 검증 가능한 자격증명(VC) 기술을 활용하여 안전하고 프라이버시 보호가 가능하며 사용자 중심의 신원관리 솔루션을 제공한다. 또한, IPFS를 블록체인 기술과 결합하여 분산 저장하고 데이터 저장 및 검색 효율성을 향상시킬 수 있다. 블록체인 기반의 분산신원관리 방안을 도입함으로써, 조직은 데이터 보안성을 높이고, 프라이버시 보호를 개선하며, 업무 프로세스를 간소화할 수 있다[11].

2.4 신원 관리에서의 IPFS

IPFS는 신원관리에 사용되는 분산파일시스템이다. 기존의 신원관리에서는 일반적으로 중앙 집

중화된 인증서버가 사용자의 신원정보를 저장하고 관리하는데 필요하다. 이 방식은 싱글 포인트 실패와 보안문제가 발생하기 쉬우므로, 분산 신원관리 방식을 사용하면 시스템의 보안성과 신뢰성이 향상된다. IPFS를 신원관리 시스템의 일부로 사용하면, 사용자의 신원정보를 분산 네트워크에 저장하여 데이터의 신뢰성과 보안성을 확보할 수 있다[12]. 또한 시스템이 더 투명하게 검증이 가능해진다. 블록체인, DID 및 IPFS를 신원관리에 사용하는 다양한 연구가 있지만, 구성원을 위한 맞춤형 통합솔루션에는 여전히 문제점이 존재한다[13].

3. 분산 신원인증 시스템

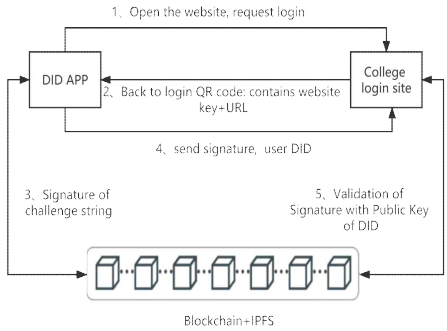
3.1 시스템 구성

시스템은 관리자, 신원 발행자, 신원 소유자, 검증 요구자 등의 역할과 관련 신원 서비스 등으로 구성된다.

관리자는 신원 발행자의 관리, 시스템의 데이터 구조, 메타데이터 의미, 알고리즘 선택, 규격 적용 및 수정, 기능 정의 등의 편성, 발행 및 반복 등을 담당한다. 신원 발행자(Issuer)는 인증기관이 담당하며, 시스템 내 사용자의 DID, VC의 초기 및 요청에 따른 생성, 발급 및 철회를 담당하며, 구성원의 신원과 탈중앙화된 디지털 신원 간의 신용 루트를 구축한다. 신원 소유자(Holder)는 디지털 신원을 가진 사용자가 담당하며, 자신의 VC와 DID 등의 관리를 담당하며, 다양한 검증 시나리오에 따라 다른 DID, VP를 독립적으로 생성하고, VC 등의 접근 권한을 부여한다. 검증 요구자(Verifier)는 디지털 신원을 가진 사용자와 시스템 응용 프로그램이 담당하며, 사용자, 주체, DID, VC, VP 등의 일관성, 완전성 및 신원 속성 정보 검증을 담당한다. 블록체인 네트워크는 탈중앙화되고 변조 방지가 가능한 데이터베이스로, DID 문서와 검증 가능한 증명서를 저장하는 데 사용된다. IPFS은 분산파일 시스템으로 인증서와 같은 신원관련 데이터를 저장하고 검색하는 데 사용된다.

3.2 분산 신원인증 등록 절차

사용자의 신원인증 로그인 프로세스는 (그림 1)과 같고 절차는 다음과 같이 진행된다.



(그림 1) Certification Registration Process

(1) 사용자는 분산신원인증 시스템 로그인 페이지를 열고, 비밀번호가 없는 인증 로그인 방식을 선택한다.
(2) 분산신원인증 시스템은 유일한 챌린지(challenge) 문자열을 생성하고, 동시에 웹 사이트의 공개키와 URL을 QR코드 형식으로 표시한다.
(3) 사용자는 자신의 DID App으로 웹 페이지에 표시된 QR 코드를 스캔하고, DID App 시스템에게 자신의 DID 정보를 보내고 임의의 도전 문자열에 서명할 수 있는 권한을 부여한다.
(4) 사용자는 자신의 서명 및 DID 정보를 분산신원인증 시스템에 전송한다.
(5) 분산신원인증 시스템은 사용자가 전송한 DID 정보와 디지털 서명을 받으면, 먼저 디지털 서명의 유효성을 검증한다.

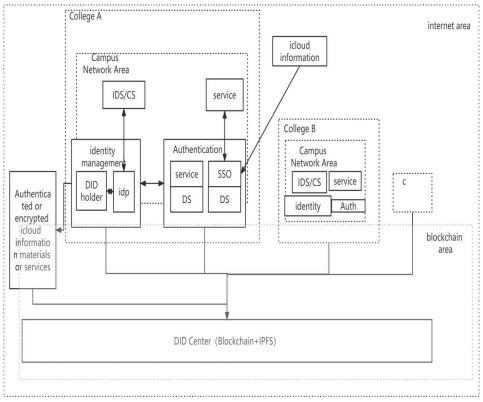
제안한 시스템은 액세스 토큰을 생성하고 사용자에게 반환한다. 사용자의 DID App은 액세스 토큰을 사용하여 IPFS 스토리지 시스템 리소스 및 서비스에 접근한다. 예를 들어, 학생 정보, 강좌 정보, 성적표 등이다. 비밀번호 없는 인증 로그인은 DID 기술과 디지털 서명 기반의 신원검증 방식이다. 이 방식은 디지털 서명 및 DID App을 사용하여 사용자 신원의 안전한 전달 및 인증을 할 수 있다. 기존의 사용자 이름 및 암호 인증방식과

비교하여, 비밀번호 없는 인증 로그인이 더 높은 보안성과 편의성을 제공하며, 동시에 신원정보 유출의 위험을 줄일 수 있다.

일반적으로 대학에서 사용하는 인증은 “사용자 이름+비밀번호” 방식이다. 이러한 인증 방식의 불편함을 해결하기 위해, QR코드 스캔으로 로그인하는 방식으로 인증 시스템을 설계한다. 블록체인 기술을 사용함으로써 사용자 신원의 고유성과 안전성을 보장할 수 있어 로그인 과정의 보안성이 향상된다. 또한, 사용자의 로그인 프로세스를 간소화하고, 탈 중앙화된 신원 식별자를 사용함으로써 싱글 포인트 실패와 공격 위험을 피할 수 있어 시스템의 신뢰성을 향상할 수 있다.

3.3 분산신원인증 시스템

분산신원인증 시스템은 블록체인 기술과 IPFS를 기반으로 한 DID 서비스를 사용하여 조직의 구성원에 대한 분산신원인증 시스템의 아키텍처를 설계한다. 분산신원인증 시스템을 분석하기 위해 조직을 대학을 대상으로 설계했다. 시스템 아키텍처는 (그림 2)와 같다.



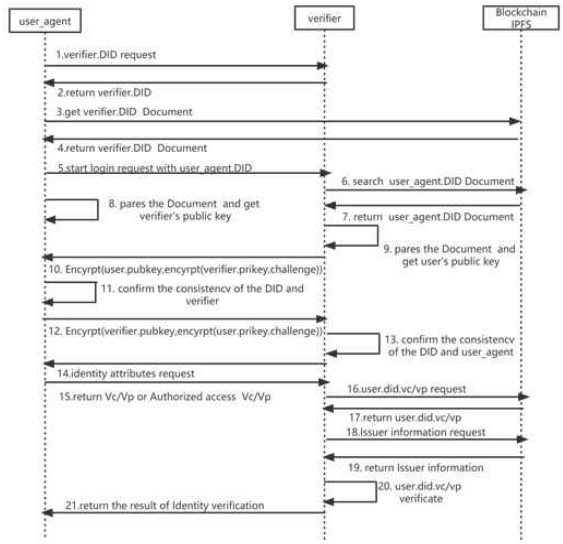
(그림 2) System Structure

(그림 2)에서 "College A, B"는 대학교의 자체 운영 정보 시스템으로 구성된 구역이고, "Campus Network Area"는 대학교의 네트워크가 커버하는 구역이다. "blockchain area"는 블록체인을 실행하고 액세스 할 수 있는 네트워크 영역을 나타낸다. "identity management", "Authentication", "신원 관리"와 "IDS /CS"는 중앙 집중식 대학 캠퍼스 네트워크 환경에서 통신하여 전통적인 시스템 간 신원정보 수집 및 공유를 구현한다.

인증 프레임 내의 SSO는 AS를 에이전트를 통해 DID, VC의 분석 및 신원정보를 얻고, DID holder, Idp, 신원인증이 있는 자료 또는 클라우드 정보는 블록체인을 통해 비즈니스 통신을 구현하고, DID center를 통해 신원정보를 공유 및 공동 유지 관리한다.

3.4 분산 신원인증 프로세스

소유자, 검증자, 저장 시스템의 시퀀스 다이어그램은 (그림 3)과 같다.



(그림 3) Sequence Diagram

(그림 3)에서, DID 프로그램 또는 DID 적용은 사용자(User_agent)와 검증자(Verifier)가 저장 시스템(Blockchain + IPFS)을 통해 신원정보를 공유하고 전달하여 인증한다. 만약 DID와 VC 데이터가 로컬에 저장되어 있다면, 인증 상호작용은 사용자와 검증자 사이에서만 이루어질 수도 있다. 10번, 12번 단계에서는 Encrypt(key, string) 함수

를 호출하여 자신의 개인키로 "도전" 정보를 암호화하고 상대방의 공개키로 암호화된 정보를 다시 암호화한 후 상대방에게 전송한다. 11번, 13번 단계에서는 Decrypt(key, string) 함수를 호출하여 공개키로 암호화된 정보를 개인키로 복호화하고, 개인키로 암호화된 "도전" 정보를 공개키로 다시 복호화해서 얻은 "도전" 정보를 바탕으로 사용자 DID의 정보 인증을 판단하고 완료한다. 16번~21번 단계에서는 신원 속성 검증을 완료하고 사용자에게 결과를 피드백 한다.

4. 분 석

분산신원기술에 기반 한 분산신원인증 시스템은 보안, 가용성 및 확장성 측면에서 분석한다.

첫 번째, 보안 측면에서 제안한 시스템은 대학 인증기관이 분산 신원 정보를 생성하고 관리하여 학생, 교수 및 직원에게 고유하고 검증 가능한 신원 표시를 제공한다. 신원 인증과정에서 DID는 검증 가능한 자격 증명(VC)을 생성하는 데 사용되어 신원 정보의 진위와 완전성을 보장한다. 사용자가 자신의 신원 정보를 완전히 소유하고 제어할 수 있도록 하여 데이터 유출 및 조작 위험을 줄일 수 있다. 제안 시스템은 분산 네트워크에 의존하여 싱글 포인트 실패가 없어 DDOS 및 DRDoS 공격에 효과적으로 대응하여 시스템의 보안성을 강화할 수 있다. DID 기술은 부분적 공개를 지원하여 사용자가 필요한 신원 정보만 공개하도록 선택할 수 있어 프라이버시를 보호하다.

두 번째, 가용성 측면에서, 제안 시스템은 DID 기술을 기반으로 다른 플랫폼 및 응용 프로그램과 통합할 수 있어 대학 구성원의 신원 인증 시스템을 보다 쉽게 배포하고 사용할 수 있다. 동시에 DID는 사용자가 필요에 따라 실시간으로 신원 정보를 업데이트할 수 있도록 하여 데이터의 정확성을 보장한다. 안정성 측면에서 DID 기술은 신원 인증 과정을 단순화하여 사용자가 디지털 신원 증명만 제공하면 되고 여러 물리적 인증서를 제공할 필요가 없다.

세 번째, 확장성 측면에서 DID 기술은 상호 안정성을 가지고 있어 다른 DID 기반 시스템과 원활한 통합이 가능하고 대학과 다른 조직간 협력을 용이하게 한다. DID 기술은 새로운 환경에 잘 적용할 수 있으며 시스템의 지속 가능한 발전. DID 기술의 모듈화 설계는 시스템이 필요에 따라 유연하게 확장할 수 있도록 하여 지속적으로 변화하는 요구를 충족시킬 수 있다.

5. 결 론

본 논문에서는 블록체인, DIDs 및 IPFS에 기반 한 탈중앙화된 분산신원인증 시스템은 조직의 신원관리에 안전하고, 확장 가능하며, 개인 정보보호를 제공하는 해결책을 제공한다.

블록체인 및 탈중앙화된 신원기술을 활용하여 신뢰할 수 있는 디지털 신원인증 생태계를 구축함으로써, 신원자기주권, 공동 유지관리, 사용자 데이터의 완전한 통제 및 선택적 공개, 탈중앙화, 비밀번호 없는 인증을 할 수 있다. 이를 통해 학습과정 데이터 기록, 성과 데이터 생성, 증명서 정보 공유 등의 응용에 대한 신용 기반을 제공한다.

향후에는 개인 정보보호를 더욱 강화하기 위한 제로 지식증명의 통합 및 기관 간 협력 및 데이터 공유를 지원하기 위해 제안된 솔루션을 확장할 예정이다.

참고문헌

[1] W3C. Decentralized Identifiers (DIDs) v1.0 [EB/OL], 2021.https: //www.w3.org/TR/did-core/.

[2] W3C.Verifiable Credentials Data Model 1.0 [EB/OL], 2019. https: //www.w3.org/TR/vc-data-model/.

[3] Zang, X., Luo, M., & Zhang, Y. “A Decentralized Identity Authentication Scheme for Higher Education Institutions Based on Blockchain”, In Proceedings of the 2020 5th International Conference on Computer and Communication Systems , pp.114-118, 2020.

[4] E. K. Jeon, S. H. Oh, D. H. Son, S. H. Lee, H. Y. Yoo & K. S. Lim, “Effects of Game Changer NFT on Metabuses”, The Journal of The Korean Institute of Communication Sciences, 39(2), pp.57-63, 2022.

[5] H. Y. Kim, K. H. Han & S. S. Shin, “A Model for Self-Authentication Based on Decentralized Identifier”, Journal of Convergence for Information Technology, 11(11), pp.66-74, 2021. https://www.w3.org/TR/vc-data-model/.

[6] J. O. Jeon & B. M. Seo, “Design and implementation of improved authentication mechanism base on mobile DRM using blockchain”, Journal of Digital Convergence, 19(4), pp.133-139, 2021.

[7] M. S. Son & H. Y. Kim, “A Self Sovereign Contents Management System based on Blockchain”, The transactions of The Korean Institute of Electrical Engineers, 70(5), pp. 784-790, 2021.

[8] Li, X., & Huang, Q, “A Decentralized Identity Management System for Higher Education Institutions Based on Hyperledger Fabric”, In Proceedings of the 3rd International Conference on Information System and Data Mining, pp.44-48, 2020.

[9] G. H. Kim, “A Design of Self-sovereign Data Distribution Platform for a Reliable Data Economy”, Journal of Digital Contents Society, 22(3), pp.483-490, 2021.

[10] W3C Verifiable Credentials Data Model v1.1, 2022.

[11] Chen, J., Xu, Q., & Zhang, X, “A University Identity Management Model Based on Blockchain and Decentralized Identifier”, In Proceedings of the 2019 International Conference on Big Data and Blockchain, pp.15-19, 2019.

[12] T. V. Doan, Y. Psaras, J. Ott. & V. Bajpai, Towards Decentralised Cloud Storage with IPFS: Opportunities, Challenges, and Future Considerations. arXiv, 2022. DOI : 10.48550/arXiv.2202.06315.

[13] Kim, H, “A Study on the Blockchain-Based Decentralized Identifier Model for the Management of University Student Records”, In Proceedings of the 2018 International Conference on Information and Communication Technology Convergence, pp. 945 - 947, 2018.

〔저자소개〕

시 정(Chai Ting)
2021년 9월 ~ 현재 : 동명대학교 컴퓨터미디어공학과 석사과정
email: me13215992762@gmail.com

신승수(Seung-Soo Shin)
2001년: 충북대학교 수학과(이학박사)
2004년 : 충북대학교 컴퓨터공학과(공학박사)
2005년 ~ 현재 : 동명대학교 정보보호학과 교수
email : shinss@tu.ac.kr

한성화(Sung-Hwa Han)
2020년 : 숭실대학교 IT정책경영학과(공학박사)
2021년 ~ 현재 : 동명대학교 정보보호학과 교수
email : shhan@tu.ac.kr