자기주권신원 및 Key Aggregate Searchable 암호를 활용한 데이터 소유자 중심의 데이터 공유 시스템

오지현, 손승환, 권덕규, 박영호

경북대학교

j2hnoh@knu.ac.kr, sonshawn@knu.ac.kr, kdk145@knu.ac.kr, parkyh@knu.ac.kr

Data Owner-Centered Data Sharing System using Self-Sovereign Identity and Key Aggregate Searchable Encryption

Oh Ji Hyeon, Son Seung Hwan, Kwon Deok Kyu, Park Young Ho

Kyungpook National Univ.

요 약

다양한 분야에서 데이터의 중요성이 증가함에 따라 이를 활용하여 서비스 개선 및 피드백 획득을 위한 요구가 증가하고 있다. 그러나 데이터에는 민감한 정보가 포함되어 있기 때문에 무분별한 데이터 사용은 보안 및 개인정보 보호 문제를 야기할 수 있다. 본 논문에서는 자기주권신원 및 key aggregate searchable 암호를 활용하여 데이터 보안 및 개인정보 보호를 보장하는 데이터 소유자 중심의 데이터 공유 시스템 모델을 제안한다.

Ⅰ. 서 론

정보통신기술의 지속적인 발전으로 인해 데이터는 다양한 산업 전반에 걸쳐 필수적인 자원으로 자리 잡았다. 데이터 분석은 기업의 핵심적인 역할을 하며, 새로운 가치를 창출하고 정보에 기반한 의사 결정을 지원하는 통찰력을 제공한다. 이에 따라 여러 산업에서는 데이터의 지속적인 수집 및 활용이 이루어지고 있다. 그러나 대부분의 데이터 관리가 중앙 집중식으로 이루어지면서, 데이터 소유자는 자신의 데이터에 대한 통제를 상실하고, 민감한 정보를 포함한 데이터의 무분별한 처리는 개인정보 침해 및 데이터 유출의 위험을 증가시킬 수 있다[1]. 또한, 데이터는 무선 네트워크를 통해 수집 및 공유되기 때문에 다양한 보안 위협에 노출될 위험이 있다[2, 3]. 이러한 문제에 대응하기 위해 접근 제어 암호 기반의 데이터 공유 시스템 연구가 수행되었지만, 제3자 의존성, 키 관리 복잡성, 데이터 검색 비효율성 등의 문제가 존재한다[4]. 이러한 문제들은 데이터의 안전성과 효율성을 저해하며, 개인정보 보호 및 데이터 관리의 효율성을 저하시킨다. 본 논문에서는 자기주권신원 및 key aggregate searchable 암호를 활용하여 데이터 소유자 중심의 안전한 데이터 공유 시스템을 제안한다. 이는 데이터 소유자의 데이터에 대한 결정권을 보유하고 개인정보를 보호하는 것을 보장한다.

Ⅱ. 배경지식

2.1. 자기주권신원

자기주권신원(Self-sovereign identity, SSI)는 개인이 자신의 디지털 신원을 직접 소유하고 관리하는 개념으로, 제3자나 중앙기관의 의존성을 없애 개인정보 보안 및 소유권 문제를 해결한다[5]. SSI는 분산식별자(Decentralized identity, DID), 검증 가능한 자격증명(Verifiable credential, VC), 검증 가능한 표현(Verifiable presentation, VP) 등을 통해 실현된다. DID는 중앙화된 권한 없이 사용자가 직접 생성하고 제어할 수 있는 고유 식별자이다. 사용자는 디지털 서명과 같은 암호화 증명을 통해 DID의 소유권을 입증하며, 블록체인에 저장 및 관리되는 DID 문서를 통해 인증을 수행한다. VC는 개인의 신원을 확인하는 자격증명으로, 특정 DID의 신뢰성을 증명하고 신뢰를 구축하기 위해 발행된다. 사용자는 VC로부터 필요한 만큼의 정보를 선택적으로 포함한 VP를 통해 자신의 신원 정보를 제3자에게 증명하거나 공유한다. SSI를 통해, 중앙 집중식 디지털 ID 관리 문제를 해결하고, 개인이 자신의 데이터를 세밀하게 제어하며, 개인 정보 보호를 촉진하고 선택적으로 공개할 수 있다.

2.2. Key Aggregate Searchable 암호

Key aggregate searchable 암호는 Cui 등이 제안한 공개키 기반 접근 제어 암호시스템으로, 여러 개의 복호 키를 하나의 단일 크기의 집계 키로 압축하여 데이터 집합을 복호화할 수 있게 제안한 기술이다[6]. 그림 1과 같이, 데이터 소유자는 자신이 공유하고자 하는 데이터 집합을 암호화한 후 클라우드 서버에 업로드한다. 그 후, 데이터 소유자는 데이터 사용자에게 권한을 부여하기 위해 해당 사용자에 대한 집계 키를 생성하고 전달한다. 데이터 사용자는 클라우드 서버로부터 받은 데이터 집합을 집계 키를 이용하여 복호화한 후 데이터를 얻을 수 있다.

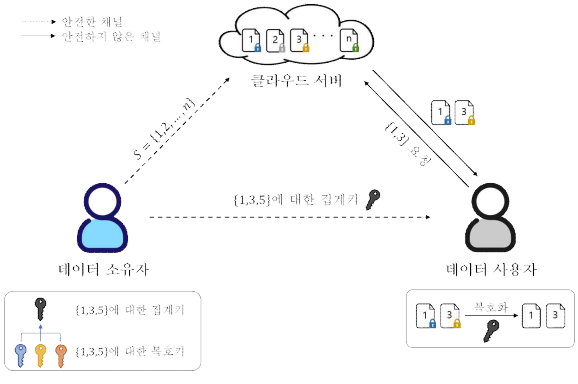

그림 1. Key aggregate searchable 암호.

Ⅲ. 제안 시스템 모델

제안하는 데이터 소유자 중심의 데이터 공유 시스템은 그림 2와 같으며, 이에 대한 구성 및 동작은 다음과 같다.

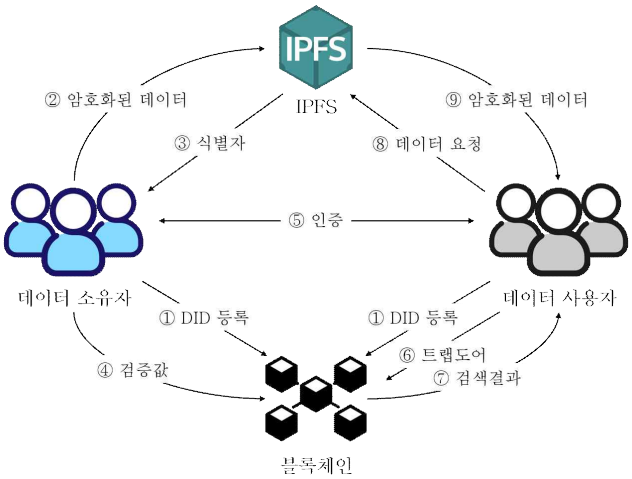

그림 2. 시스템 모델.

3.1. 시스템 구성

제안하는 시스템은 데이터 소유자, 데이터 사용자, 블록체인 및 IPFS(Interplanetary file system)로 구성되며, 각 개체에 대한 설명은 다음과 같다.

- 데이터 소유자: 데이터 소유자는 자신의 데이터에 대한 시스템 매개변수를 생성하며, 암호화된 데이터를 IPFS를 통해 관리한다. 데이터 소유자는 블록체인에 저장된 DID 문서를 통해 데이터 사용자 검증을 수행하여 접근 권한을 부여한다.
- 데이터 사용자: 데이터 사용자는 데이터 소유자로부터 발급받은 VC를 통해 데이터 접근 권한을 얻는다. 데이터 사용자는 VP 및 트랩도어를 통해 블록체인으로부터 반환된 식별자를 이용하여 IPFS로부터 데이터를 얻는다.
- 블록체인: 데이터 사용자로부터 받은 VP의 정확성을 검증한 후 트랩도어를 통해 일치하는 식별자를 반환한다.
- IPFS: 데이터 소유자가 데이터 저장을 위해 활용하는 P2P 분산형 데이터베이스로, 데이터의 식별자를 기반으로 데이터 저장 및 검색을 가능한 분산형 및 콘텐츠 주소 지정 스토리지 시스템이다.

3.2. 시스템 동작

제안 시스템은 9단계로 동작하며, 각 단계에 대한 설명은 다음과 같다.

1) 데이터 소유자 및 데이터 사용자는 데이터 소유자가 생성한 시스템 매개변수를 사용하여 공개키 및 개인키 쌍을 생성한 후, DID 문서를 생성하여 블록체인에 등록한다.
2) 데이터 소유자는 데이터 암호화 수행 후 IPFS에 업로드한다.
3) IPFS는 수신받은 데이터에 대한 식별자를 생성하고 이를 데이터 소유자에게 전달한다.
4) 데이터 소유자는 데이터로부터 키워드를 추출한 후 검증값을 생성하여 블록체인에 업로드한다.
5) 데이터 사용자는 데이터 소유자에게 데이터 접근 권한을 요청한다. 각 개체는 DID를 통한 상호인증을 수행하고 데이터 소유자는 접근 허가로서 집계 키 및 VC를 발행한다.
6) 데이터 사용자는 원하는 데이터에 대한 키워드를 사용하여 트랩도어를 생성한 후 VP와 함께 블록체인으로 검색 쿼리를 보낸다.
7) 블록체인은 데이터 사용자를 검증한 후 검색 결과를 반환한다.
8) 데이터 사용자는 검색 결과로부터 얻은 식별자를 이용하여 IPFS에게 데이터를 요청한다.
9) IPFS는 일치하는 암호화된 데이터를 전달하며, 데이터 사용자는 집계 키를 통해 데이터를 복호화하고 데이터 무결성을 검증한다.

Ⅳ. 결론

데이터에 대한 중요성이 확대됨에 따라 산업 전반에서 데이터 수집 및 공유의 필요성이 증가하고 있다. 이에 따라 안전한 데이터 공유를 위한 연구가 이루어지고 있지만 기존 연구들은 제3자에 대한 의존성, 키 관리의 복잡성, 데이터 검색의 비효율성 등의 문제가 존재한다. 따라서 본 논문에서는 자기주권신원 및 key aggregate searchable 암호를 활용하여 데이터 소유자가 자신의 데이터를 자기주도적으로 관리하고 공유할 수 있는 시스템을 제안하였다. 향후 제안한 시스템 모델을 통해 안전한 데이터 공유를 위한 프로토콜 방식이 제안 가능하다.

ACKNOWLEDGMENT

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.RS-2024-00396797, Development of core technology for intelligent O-RAN security platform)

참 고 문 헌

[1] Lee, J., Oh, J., Kwon, D., Kim, M., Kim, K., and Park, Y. “Blockchain-enabled key aggregate searchable encryption scheme for personal health record sharing with multi-delegation,” IEEE Internet of Things Journal, 2024.

[2] Yu, S., Das, A. K., Park, Y., and Lorenz, P. “SLAP-IoD: Secure and lightweight authentication protocol using physical unclonable functions for internet of drones in smart city environments,” IEEE Transactions on Vehicular Technology, pp. 10374-10388, Jul. 2022.

[3] Park, K. and Park, Y. “IAKA-CIOT: An improved authentication and key agreement scheme for cloud enabled internet of things using physical unclonable function,” Sensors, pp. 6264-6282, Aug. 2022.

[4] Oh, J., Lee, J., Kim, M., Park, Y., Park, K., and Noh, S. “A secure data sharing based on key aggregate searchable encryption in fog-enabled IoT environment,” IEEE Transactions on Network Science and Engineering, pp. 4468-4481, Nov.-Dec. 2022.

[5] Hong S and Kim H. “VaultPoint: A blockchain-based SSI model that complies with OAuth 2.0,” Electronics. pp. 1231-1250, Jul. 2020.

[6] Cui, B., Liu, Z., and Wang, L. “Key aggregate searchable encryption (KASE) for group data sharing via cloud storage,” IEEE Transactions on Computers, pp. 2374-2385, Jan. 2016.