민감정보 삭제권 보장을 위한 절차 원장 기반 블록체인 및 오프체인 관리 시스템

신희재[1], 이재민[2], 김동성*

금오공과대학교 IT융복합공학과[1,2,*]

{shinheejae[1], ljmpaul[2], dskim*}@kumoh.ac.kr

A Procedure-Ledger Blockchain with Off-Chain Management for Sensitive Data Deletion

Hee-Jae Shin[1], Jae-Min Lee[2], Dong-Seong Kim*

Kumoh National Institute of Technology, Dept. of IT Convergence Eng.[1,2,*]

요 약

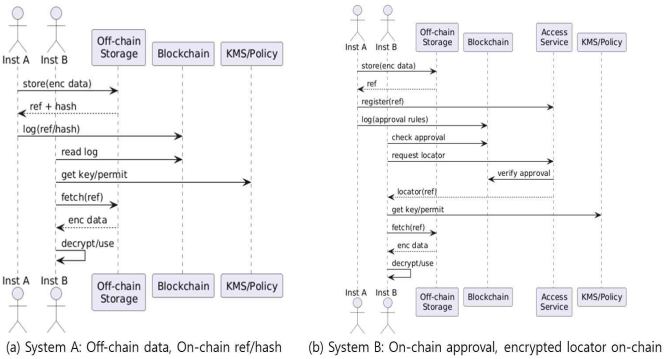
본 논문은 블록체인을 민감 정보의 직접적인 저장소가 아닌, 데이터 생애주기 전반의 이벤트를 기록하는 불변 절차 원장(Immutable Procedure Ledger, IPL)으로 활용하는 설계를 제안한다. 민감정보 본문은 오프체인 저장소(Off-chain Storage, OCS)에 암호화하여 저장하며, 온체인에는 난수 기반 레코드 식별자(Random Record Identifier, RRID)와 최소한의 절차 로그만을 남긴다. 오프체인 객체 조회를 위한 로케이터(Locator, LOC)는 온체인에 노출하지 않고 보관 기관 내부의 식별자 매핑(Identifier Map, IM)에서 'RRID → LOC' 형태로 관리하며, 접근 승인 시에만 로케이터 엔벨로프(Locator Envelope, LE)를 통해 해당 당사자에게 제한적으로 전달한다. 삭제 요청 시에는 보관 기관이 LOC에 대응하는 오프체인 객체를 제거하고, 다수 주체의 서명 기반 삭제 증빙(Attestation)을 수집해 온체인에 기록함으로써 절차의 최종 완료를 검증 가능하게 한다. 본 방식은 온체인에 참조 흔적을 남기지 않으면서도, 다기관 환경에서 투명한 접근 및 삭제 이력 관리를 지원하는 것을 목표로 한다.

Ⅰ. 서 론

디지털 전환이 가속화됨에 따라 개인정보를 포함한 각종 민감정보의 안전한 관리와 유통은 현대 사회의 핵심적인 과제가 되었다. 특히 의료와 같이 정보의 민감도가 높은 산업군에서는 블록체인의 분산 아키텍처가 보안성을 혁신할 것이라는 긍정적인 전망이 존재한다[1]. 최근에는 장기 이식 매칭 분야에서 실제 식별 정보 대신 블록체인 주소를 매칭 식별자로 활용함으로써 개인정보 노출을 최소화하려는 시도도 이루어지고 있다[2]. 그러나 불변성이라는 블록체인의 본질적 특성은 GDPR 등에서 요구하는 개인정보 삭제 권리와 충돌할 수 있다. 특히 해시 값조차 개인정보로 간주될 수 있는 규제 환경에서는 데이터만을 오프체인에 분리하는 기존 방식으로는 충분하지 않을 수 있다. 이러한 문제를 완화하기 위해 본 논문은 블록체인을 절차 이벤트만 기록하는 불변 절차 원장(Immutable Procedure Ledger, IPL)으로 한정하고, 온체인에는 난수 기반 레코드 식별자(Random Record Identifier, RRID)와 최소 로그만 남기는 설계를 제안한다. 민감 정보 본문은 오프체인 저장소(Off-chain Storage, OCS)에 암호화하여 저장하며, 객체 조회를 위한 로케이터(Locator, LOC)는 기관 내부의 식별자 매핑(Identifier Map, IM)에서 'RRID → LOC' 형태로 은닉 관리한다. 나아가, 승인된 수신자에게만 LOC를 안전하게 전달하기 위해 로케이터 엔벨로프(Locator Envelope, LE) 기반의 암호화 교류 메커니즘을 제안함으로써 온체인 상의 참조 흔적을 원천적으로 차단하고자 한다.

Ⅱ. 기존 시스템

민감정보를 온체인에 직접 저장하지 않기 위해 기존 연구들은 대개 오프체인 저장소(OCS)에 원문을 보관하고, 블록체인에는 접근 제어 정책, 감사 로그, 무결성 검증용 해시값과 함께 오프체인 객체를 식별하기 위한 참조 정보(Reference)를 기록하는 방식을 취해 왔다[3, 4]. [그림 1(a)]와 같은 대표적인 하이퍼레저 패브릭 기반의 속성 기반 액세스 제어(ABAC) 설계에서는 암호화된 데이터를 IPFS에 저장한 뒤, IPFS가 반환하는 리소스 주소(Content ID)와 관련 정책 정보를 원장에 기록하여 데이터 공유의 투명성을 확보한다[3]. 또한, 유전체 데이터 공유 시스템인 ConsentChain의 경우, 데이터 참조(DRef) 및 메타데이터를 포함한 스마트 컨트랙트를 통해 데이터 주권과 감사 추적성을 구현한다[4]. 이러한 구조는 기관 간 데이터 검증이 용이하다는 장점이 있으나, 온체인에 남겨진 참조 정보가 데이터의 위치나 특정 프로파일과 결합될 경우 장기적인 링크 가능성(Linkability)을 유발하여 참조 흔적이 남을 수 있다. 온체인 참조 노출에 따른 프라이버시 위험을 줄이기 위해, [그림 1(b)]와 같이 참조 정보를 직접 노출하는 대신 암호화된 포인터를 활용하거나 일회성 접근 제약을 부여하는 방식도 제안되었다. 이는 데이터 공유 요청이 승인되면 제공자가 임시 저장소에 일회성 객체를 생성하고 그 접근 URL을 수신자의 공개키로 암호화하여 블록체인에 기록하며, 사용 후에는 해당 객체를 제거하여 URL을 무력화하는 방식이다[4]. 그러나 이 역시 참조 정보를 온체인에서 완전히 제거하는 것이 아니라 암호화하여 잔존시키는 방식에 해당하며, 만료 및 재발급을 위한 추가적인 운영 로직과 신뢰 경계 확장이 불가피하다는 한계가 있다.



(a) System A: Off-chain data, On-chain ref/hash (b) System B: On-chain approval, encrypted locator on-chain

그림 1 기존 블록체인-오프체인 연동 기반의 참조 기록 방식

Ⅲ. 제안하는 시스템

본 논문은 블록체인을 민감 정보의 직접적인 저장소나 참조 공유 수단이 아닌, 데이터 생애주기 전반의 절차 이벤트를 기록하는 불변 절차 원장(IPL)으로 정의한다. 실제 민감 정보는 오프체인 저장소(OCS)에 암호화되어 저장되며, 온체인에는 데이터 본문, 개인 식별자, IPFS CID와 같은 저장 참조인 LOC를 일절 기록하지 않는다. 대신 [그림 2]와 같이 등록(Record Registered), 접근 요청/승인(Access Granted), 삭제 요청/승인(Delete Approved), 증빙 제출(Submit Attestation), 삭제 최종화(Delete Finalized) 등 무결성 검증에 필요한 절차 로그만을 남긴다.

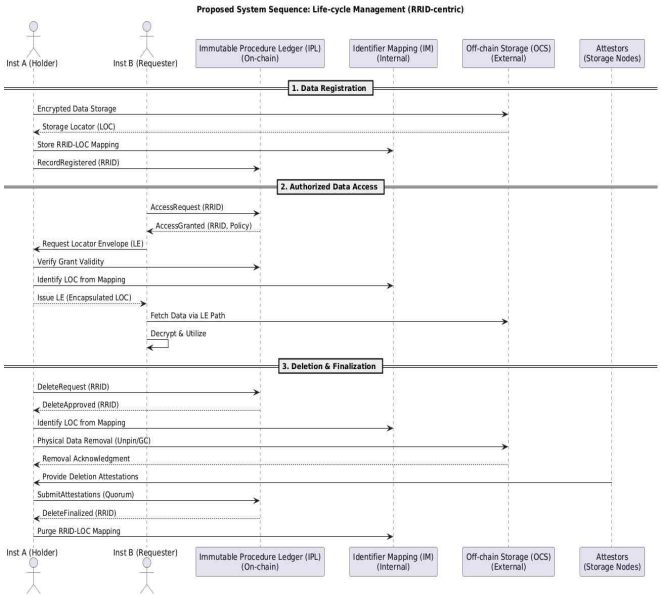


그림 2 RRID 기반 불변 절차 원장(IPL)의 생애주기별 처리 시퀀스

이 구조의 핵심은 난수 기반 레코드 식별자(RRID)를 활용한 비식별 식별 체계이다. RRID는 온체인에서 레코드를 지칭하는 키로 사용된다. 데이터 보관 기관은 민감 정보를 OCS에 저장한 후 획득한 LOC를 온체인에 노출하는 대신, 기관 내부의 식별자 매핑(IM)에 'RRID → LOC' 형태로 은닉 관리한다. 데이터 접근 요청 시 보관 기관은 [그림 3(a)]에 명시된 절차에 따라 온체인의 승인 이벤트를 대조하여 유효성을 검증한다. 이후 내부 매핑(IM)에서 조회한 LOC 및 정책 정보를 포함하여 로케이터 엔벨로프(LE)를 생성한다. LE는 수신자의 공개키로 암호화되고 발급자 서명이 부가된 보안 객체로, 온체인에 노출되지 않는 오프체인 보안 채널을 통해 전달된다. 이를 통해 시스템은 온체인에 조회 흔적을 남기지 않으면서 권한이 확인된 사용자에게만 안전하게 접근 경로를 제공한다. 데이터 삭제 또한 RRID를 기준으로 수행되어 블록체인의 불변성과 사용자의 삭제 권리를 동시에 충족한다.

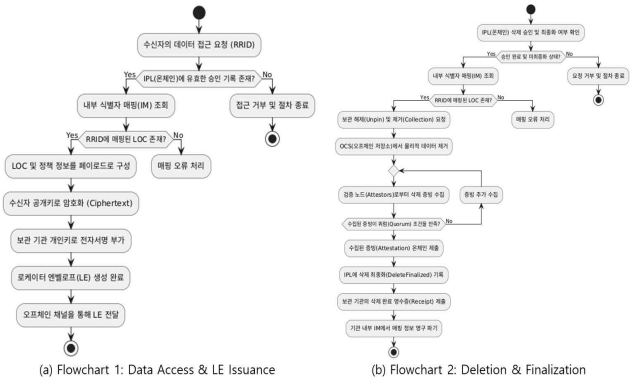


그림 3 데이터 생애주기 단계별 상세 플로우차트

[그림 3(b)]는 삭제 승인 확인부터 최종화에 이르는 전 과정을 나타낸다. IPL에 삭제 승인이 기록되면 보관 기관은 대상 LOC를 확인하여 OCS에서 객체를 물리적으로 제거하고, 보관 해제(Unpin) 및 가비지 컬렉션을 요청한다. 이후 저장 노드 등 운영 주체는 삭제 수행 사실을 서명 기반 삭제 증빙(Attestation)으로 생성하며, 보관 기관은 이를 수집하여 쿼럼(Quorum) 조건을 검증한다. 정의된 쿼럼이 충족되면 IPL에 최종 삭제 완료 상태(DeleteFinalized)를 기록하고, 보관 기관은 내부 매핑 정보(IM)를 영구 파기하여 온체인과 오프체인 간의 연결 고리를 원천 차단한다. 이러한 설계는 다수 주체의 합의를 통해 삭제 행위의 신뢰성을 객관적으로 증명한다.

Ⅳ. 결 론

본 논문은 민감 정보 교류 시 블록체인의 불변성과 삭제 권리가 충돌하는 문제를 해결하고자 RRID 중심의 IPL 설계를 제안하였다. 제안 시스템은 온체인에 LOC를 기록하는 대신 기관 내부 IM에 은닉하고, 승인된 교류 시에만 LE를 통해 전달함으로써 온체인 참조 잔존 문제를 원천 차단하였다. 이를 통해 삭제 후에도 남는 링크 가능성을 제거하고 절차적 무결성을 확보하였다. 향후 연구로는 첫째, 환자 동의 기반의 의료 데이터 교류 환경을 고려하여 동의 메커니즘과의 연동을 고도화할 필요가 있다. 둘째, LE 전달 과정에서 중앙 서버 의존에 따른 집중화 문제를 방지하기 위해, 노드 간 P2P 연결을 통한 직접적인 정보 교환 및 복원력 확보 방안을 연구해야 한다. 셋째, 삭제 증빙의 신뢰도를 높이기 위해 다양한 참여 주체를 포함하는 쿼럼 규칙과 감사 수준에 따른 최종화 조건을 구체화하여 절차 중심의 프라이버시 보호 모델을 완성하고자 한다.

ACKNOWLEDGMENT

본 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 지역지능화혁신인재양성사업(IITP-2025-RS-2020-II201612, 25%)과 2025년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(2018R1A6A1A03024003, 25%)과 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-학·석사연계 ICT 핵심인재양성 지원(IITP-2025-2022-00156394, 25%)과 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터사업의 연구결과로 수행되었음(IITP-2025-RS-2024-00438430, 25%)

참 고 문 헌

[1] S. O. Ajakwe, I. I. Saviour, V. U. Ihekoronye, O. U. Nwankwo, M. A. Dini, I. U. Uchechi, D.-S. Kim, and J.-M. Lee, "Medical IoT Record Security and Blockchain: Systematic Review of Milieu, Milestones, and Momentum," Journal of Information Security and Applications, Vol. 8, No. 9, pp. 1-28, Sep. 2022

[2] I. S. Igboanusi, C. A. Nnadiekwe, J. U. Ogbede, D.-S. Kim, A Lensky, "BOMS: blockchain-enabled organ matching system," Scientific Reports, Vol. 14, No.1, pp. 1-13, July 2024

[3] X. Zhao, S. Wang, Y. Zhang, and Y. Wang, "Attribute-based access control scheme for data sharing on hyperledger fabric," Journal of Information Security and Applications, Vol. 67, pp. 1-16, Jun. 2022

[4] F. Albalwy, A. Brass, and A. Davies "A Blockchain-Based Dynamic Consent Architecture to Support Clinical Genomic Data Sharing (ConsentChain): Proof-of-Concept Study," JMIR Medical Informatics, Vol. 9, No. 11, pp. 1-24, Nov. 2021