

하이퍼레저 패브릭과 DID를 사용한 EMR관리 시스템 기법 제안

엄효상¹, 강혁², 이근호¹

¹백석대학교 컴퓨터공학부

²고려대학원 영상정보처리협동과정

djagytkd0925@naver.com, kanghyeok74@bu.ac.kr, root1004@bu.ac.kr

EMR Management System Using Hyperledger Fabric and DID

Hyo-sang Eom¹, Hyeok Kang², Keun-Ho Lee¹

¹Div. of Computer Engineering, Baek-seok University

²Program. in Visual Information Processing, Korea University

요 약

EMR 시스템은 환자들의 진료, 처방 및 개인정보들을 중앙집중형으로 관리하는 시스템이다. 기존 EMR 시스템은 수기로 작성하던 진료기록을 컴퓨터를 통해 전자문서 형태로 관리하고 있다. 그러나 EMR 시스템은 외부로부터 해킹이나 데이터 유출에 대한 피해가 우려된다. 본 논문에서는 블록체인 기반의 하이퍼레저 패브릭과 DID를 사용하여 EMR 데이터를 분산 저장하여 환자의 진료기록을 안전하게 관리하는 시스템 기법을 제안한다.

1. 서론

현재 국내 병원에서는 종이 문서에 대한 분실, 훼손 등의 이유로 종이에 기록된 환자의 진료 및 의료 기록을 전자문서 형태로 저장하고 보존하는 EMR(Electronic Medical Record) 시스템을 사용한다. 그러나 EMR에 저장된 데이터들은 일반적으로 중앙 집중형 방식으로 저장되고 있다. 이는 외부로부터의 해킹과 환자의 신원정보 및 데이터의 유출로 이어질 수 있다. 또한 환자들의 진료 및 처방 기록이 조작될 우려가 있고 외부의 공격으로 서버가 마비되는 심각한 피해를 볼 수 있다.

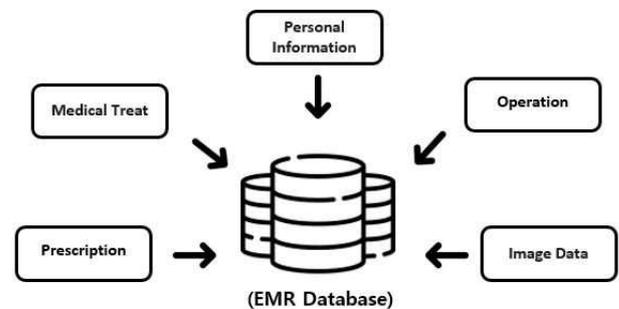
본 논문에서는 기존의 중앙집중형 EMR 시스템으로 인해 예견될 수 있는 해킹, 데이터 유출 등을 방지하고자 하이퍼레저 패브릭과 DID 기술을 사용하여 안전하게 EMR을 관리하는 기법을 제안한다. 하이퍼레저 패브릭을 사용하여 허가된 사용자만 환자의 진료기록을 개방할 수 있도록 하고, DID 기술을 통해 더욱 안전한 신원 인증을 할 수 있도록 한다.

2. 관련연구

2.1 EMR

EMR(Electronic Medical Record)은 환자들의 치료 및 처방, 진료에 따른 기록을 전자적 형태로 기록해

놓은 것을 의미한다. 의료기관에서는 종이로 환자들의 기록이 관리가 되었던 형태가 개인용 PC가 보급되기 시작한 1990년대 중반 이후부터 IT 기술과 접목하여 병원에서 핵심기술로 쓰이고 있다.



(그림 1) EMR의 저장구조.

2.2 하이퍼레저 패브릭(Hyperledger Fabric)

하이퍼레저 패브릭(Hyperledger Fabric)은 분산 원장 기술인 블록체인의 일종으로, 허가형 분산 원장 기술(DLT, Distributed Ledger Technology) 플랫폼으로 사용되고, 블록체인 플랫폼 또는 다른 분산 원장과 차별화되는 주요 기능을 제공한다[1]

2.2.1 체인코드(Chain code)

하이퍼레저 패브릭의 체인코드는 비즈니스 로직을 구성원들의 동의로 처리하기 때문에 스마트 계약으

로 생각할 수 있다[2].

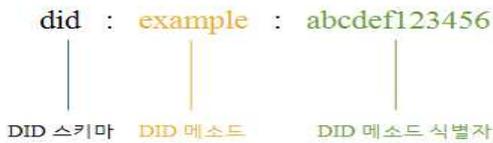
체인코드는 계약으로써 외부로부터의 계약에 대해서 이상이 없는지 비교와 검증을 통해 결과를 원장에 기록하게 동작한다.

2.3 DID

DID(Decentralized Identity)는 블록체인 기반의 중앙화 된 기관이 필요 없이 탈중앙화 환경에서 사용자의 신원을 인증할 수 있도록 구현된 기술이다. 여러 국가와 기관 등에 분산되어 탈중앙화 되어 중앙 등록 기관 없이 자기 주권 신원 증명체계를 말한다[3].

자격증명이 필요한 경우 VC(Verifiable Credential)를 저장한 뒤 원하는 정보만 자신이 선택해 제출할 수 있다. DID는 블록체인 기술을 기반으로 하기에 데이터의 변조에 대한 위협이 적고 데이터들을 암호화하여 저장해 보안 위협으로부터 안전하다.

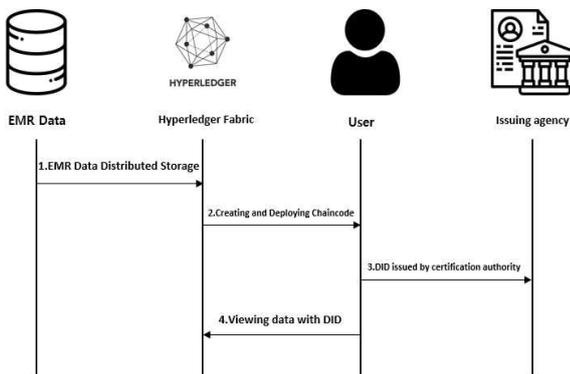
아래 그림은 DID의 형식에 대한 식별구조이다.



(그림 2) DID 식별구조

3. 제안 기법

본 논문에서 제안하는 기법은 하이퍼레저 패브릭과 공개키 암호 알고리즘을 사용하여 안전하게 EMR 데이터를 분산 저장하고 DID를 사용하여 데이터를 열람하는 기법을 제안한다.



(그림 3) 시스템제안

Step1. EMR 데이터들을 공개키 암호 알고리즘으로 암호화하여 하이퍼레저 패브릭에 안전하게 분산 저장한다.

Step2. 하이퍼레저 패브릭에서 병원 관리자 및 환자

에게 참여를 위한 체인코드를 생성한다.(참여자 초대하여 패브릭 구성)

Step3. 병원 관리자, 환자는 DID를 발급기관으로부터 발급받는다. 이때 참여자별로 권한을 두어 접근할 수 있는 데이터를 제한한다.

Step4. 자신이 발급받은 DID를 환자들의 분산 저장된 기록을 열람할 때 개인 키를 가지고 복호화한 뒤 개인 DID를 입력하여 EMR 데이터들을 열람하게 된다.

5. 결론

본 논문에서는 기존의 EMR 데이터들이 중앙집중형 방식으로 저장되어 외부로부터의 해킹과 조작, 유출 등의 취약점을 방지하고자 하이퍼레저 패브릭 기술과 DID를 사용해서 EMR 시스템을 관리하는 기법을 제안했다.

현재 블록체인을 통한 EMR 시스템에 대한 연구가 활발히 진행 중이며, 의료정보는 보안성이 요구되는 민감한 정보이기 때문에 법적 문제가 우려될 수 있어 취급에 주의가 필요하다.

감사의 글

본 논문은 2020년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(NRF-2020R111A3069008)

참고문헌

[1] Hyperledger Fabric, (internet), <https://hyperledger-fabric.readthedocs.io/en/release-2.5/whatis.html>.

[2] Won-Yong Hwang, Hyo-Kwan Kim, A Study on Implementation of Blockchain Voting System using Hyperledger Fabric, The Korea Institute of Information, Electronics, and Communication Technology, vol.13, no.4, pp. 298-305, 2020.

[3] Hye-Won Kim, Young-Eun Lee, Min-Ho Kwon, Myung-Joon Lee, BCON : Blockchain-based Content Management Service Using DID, The Korean Society Of Computer And Information, 97-105, 2021.