블록체인 기반의 접근 제어를 제공하는 안전한 전자 의료 기록 공유 시스템 설계

손승환, 김명현, 이준영, 박영호

경북대학교

sonshawn@knu.ac.kr, kimmyeong123@knu.ac.kr, harry250@knu.ac.kr, parkyh@knu.ac.kr

Secure Electronic Health Record Sharing System With Blockchain-Based Access Control

Son Seung Hwan, Kim Myeong Hyun, Lee Joon Young, Park Young Ho

Kyungpook National Univ.

요 약

전자 의료 기록은 환자의 민감한 정보를 포함할 수 있어 안전한 공유 시스템이 필요하다. 최근 클라우드 기반의 전자 의료 기록 공유 시스템이 연구되고 있으나 클라우드는 단일 실패지점이 존재하여 시스템의 안전성을 보장할 수 없다. 블록체인은 클라우드의 중앙 집중화된 문제를 해결할 수 있는 분산원장기술이며 저장된 정보의 무결성 및 투명성을 보장할 수 있다. 본 논문에서는 블록체인 기반의 접근 제어를 제공하는 안전한 전자 의료 기록 공유 시스템을 설계하였다.

Ⅰ. 서 론

정보통신기술의 발전으로 인해 종이 기반의 의료 기록 보관이 전자 의료 기록으로 대체되었다. 전자 의료 기록에는 질병 이름과 진단 기록 등의 정보가 포함된다. 의사 또는 의료기관은 전자 의료 기록을 공유하여 더 나은 치료법을 개발할 수 있고 환자는 질 좋은 의료 서비스를 제공받을 수 있다. 하지만 전자 의료 기록은 환자의 민감한 정보를 포함할 수 있으며 [1] 공격자에 의해 의료 기록이 유출될 경우 이는 심각한 물적 및 인적 피해를 유발할 수 있다. 그러므로 안전한 전자 의료 기록 공유 시스템이 필요하며 최근 클라우드 기반의 전자 의료 기록 공유 시스템이 활발하게 연구되고 있다[2,3]. 클라우드 기반의 시스템은 효율적으로 정보를 공유할 수 있으나 중앙화된 특징으로 인해 공격자들의 주요 목표가 될 수 있으며 [4] 단일 실패 지점 문제가 발생할 수 있다. 따라서 분산화된 전자 의료 기록 공유 시스템이 필요하며 안전하고 효율적인 접근 제어 정책이 필요하다.

본 논문에서는 클라우드 기반 시스템의 문제점을 해결하기 위해 블록체인 기반의 접근 제어를 제공하는 안전한 전자 의료 기록 공유 시스템을 설계한다.

Ⅱ. 제안 시스템

본 논문에서 제안하는 시스템 모델은 그림 1과 같다. 제안 모델은 신뢰기관, 환자, 병원, 사용자 및 블록체인으로 구성된다.

- 신뢰 기관은 시스템의 공개 키를 배포하고 병원에 대한 공개키 쌍을 생성한다. 또한 사용자 등록과정에서 속성 키를 분배하고 사용자의 ID와 속성 값을 블록체인에 저장한다.
- 환자는 자신의 의료 기록에 대한 접근 트리를 설정하며 블록체인에 저장하기 위한 서명 값을 생성한다. 추후 자신의 의료 기록이 공유되면 블록체인을 통해 이를 확인할 수 있다.

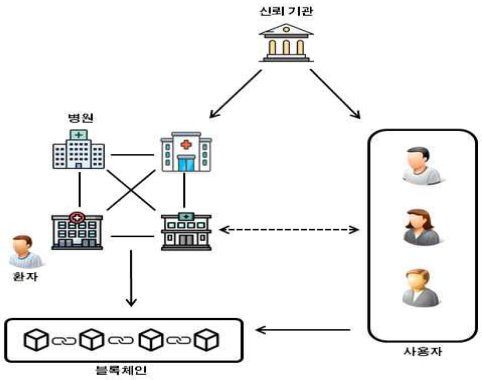

그림 1. 블록체인을 활용한 전자 의료 기록 공유 시스템 모델.

- 병원은 전자 의료 기록을 저장하며 분산 원장을 유지한다. 자신의 데이터베이스에 저장되어 있는 전자 의료 기록에 대한 접근 트리, 해시, 병원의 주소를 포함한 트랜잭션을 생성한다. 사용자가 의료 기록을 요청하면 해당 사용자가 가지고 있는 속성 값이 암호문의 접근 트리를 만족하는지 확인 후 의료 기록을 전송한다. 의료 기록을 전송한 후 그에 따른 해당 암호문의 해시, 병원의 주소, 사용자의 서명 값을 포함하는 트랜잭션을 블록체인에 업로드한다.
- 사용자는 블록체인을 통해 병원이 기록한 트랜잭션을 확인할 수 있다. 정부 직원 또는 의료 연구원이 사용자에 포함될 수 있으며, 등록과정에서 받은 속성 키가 트랜잭션에 기록된 접근 트리를 만족할 경우 병원의 주소로 해당 의료 기록을 요청할 수 있다.
- 블록체인은 병원과 신뢰 기관에 의해 유지되며 트랜잭션이 생성 및 합의된다. 블록체인에 저장되는 정보는 사용자의 ID와 속성값, 각 병원에서 생성된 전자 의료 기록에 대한 트랜잭션, 공유된 의료 기록에 대한

트랜잭션이 포함된다. 환자와 사용자는 새로운 트랜잭션을 생성할 권한은 없으나 블록체인의 원장에 접근할 수 있다. 환자의 경우 자신의 의료 기록에 대한 공유 여부를 확인할 수 있고 사용자는 의료 기록에 대한 접근 트리와 병원 주소 또는 병원으로부터 받은 암호문에 대해 무결성을 검증할 수 있다.

Ⅲ. 제안 프로토콜

제안 프로토콜에서 사용된 기호는 표 1과 같다.

표 1. 사용된 기호

기호	의미
H_j	j번째 병원
P_k	k번째 환자
U_i	i번째 사용자
P_{TA}, P_j	TA 및 H_j의 공개 키
$h(.)$	해시 함수 $h(.):\{0,1\}^*\rightarrow Z_q$
$H(.)$	해시 함수 $H(.):\{0,1\}\rightarrow G_1$
ID_j	H_j의 아이디
s_j	H_j의 개인 키
add_j	H_j의 주소 값
ATT_i	U_i의 속성 집합
A_{i_x}, A'_{i_x}	U_i의 속성 키
EHR_k	P_k의 전자 의료 기록
Γ_k	EHR_k에 대한 접근 트리
γ	Γ_k의 루트 노드
CT_k	암호화된 EHR_k
SK	H_j와 U_i의 세션 키

3.1. 전자 의료 기록 저장

환자가 자신의 EHR_k에 대한 접근 트리 Γ_k를 설정한다. 이후 병원은 Γ_k에 따라 EHR_k를 암호화한 후 암호문은 데이터베이스에 저장하고 접근 트리, 해시값, 병원의 주소 값, 서명 값을 블록체인에 저장한다. 제안한 전자 의료 기록 저장 프로토콜은 그림 2와 같다.

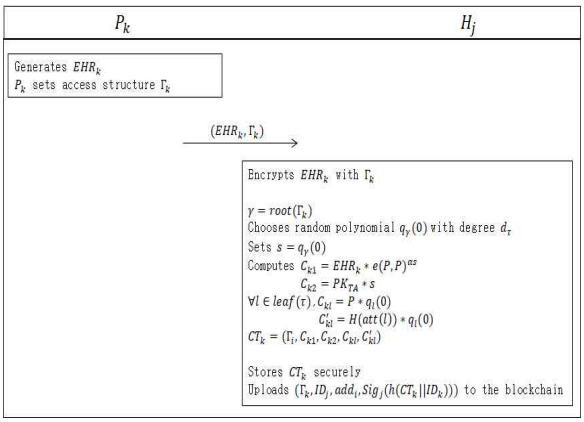

그림 2. 제안한 전자 의료 기록 저장 프로토콜.

3.2. 전자 의료 기록 공유

사용자가 병원에 전자 의료 기록을 요청하면 병원과 사용자는 상호 인증후 세션 키 SK를 생성한다. 이후 병원은 암호화된 전자 의료 기록을 전송하고 사용자는 자신이 가진 속성 키를 사용하여 전자 의료 기록을 해독할 수 있다. 제안한 전자 의료 기록 공유 프로토콜은 그림 3과 같다.

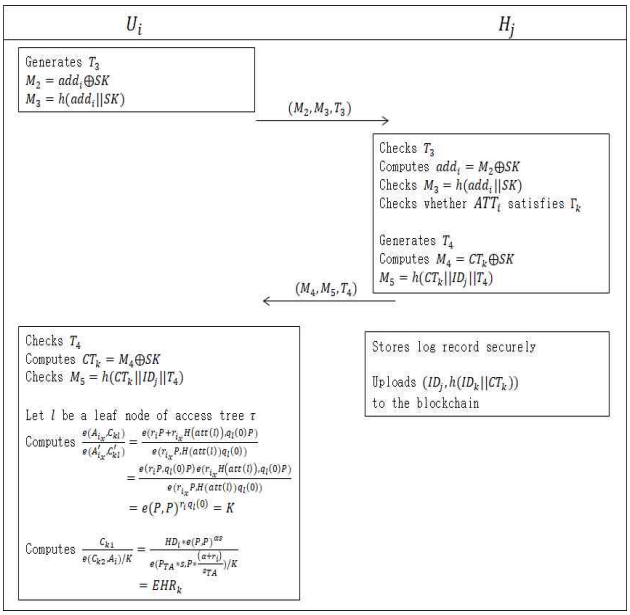

그림 3. 제안한 전자 의료 기록 공유 프로토콜.

Ⅳ. 결론

본 논문에서는 블록체인 기반의 접근 제어를 제공하는 전자 의료 기록 공유 시스템을 설계하였다. 제안한 시스템은 클라우드를 사용하지 않고 각 병원에 의료 기록을 저장함으로써 단일 실패 지점 문제를 해결하였으며 병원에 저장된 정보에 대한 접근 트리, 해시, 주소 등을 블록체인에 기록하여 전자 의료 기록에 대한 무결성을 보장하고 접근 제어를 실현할 수 있다.

참 고 문 헌

[1] Park, K., Noh, S., Lee, H., Das A. K., Kim, M., and Park, Y. "LAKS-NVT: Provably Secure and Lightweight Authentication and Key Agreement Scheme Without Verification Table in Medical Internet of Things," IEEE Access, vol. 8, pp. 119387-119404, 2020.

[2] Kim, M., Yu, S., Lee, J., Park, Y., and Park, Y. "Design of Secure Protocol for Cloud-Assisted Electronic Health Record System Using Blockchain," Sensors, vol. 20, no. 10, p. 2913, 2020.

[3] Son, S., Lee, J., Kim, M., Das A. K., and Park, Y. "Design of Secure Authentication Protocol for Cloud-Assisted Telecare Medical Information System Using Blockchain," IEEE Access, vol. 8, pp. 192177-192191, 2020.

[4] Park, Y., and Park, Y. "Three-Factor User Authentication and Key Agreement Using Elliptic Curve Cryptosystem in Wireless Sensor Networks," Sensors, vol. 16, no. 12, p. 2123, 2016.

[5] Nakamoto S. "Bitcoin: A Peer-to-Peer Electronic Cash System," Bitcoin.org, 2008, (http://bitcoin.org/bitcoin.pdf).

[6] Bethencourt, J., Sahai, A., and Waters, B. "Ciphertext-Policy Attribute-Based Encryption," Proceeding of IEEE Symposium on Security and Privacy (SP), May. pp. 321-334., 2007.