환자의 익명성이 보장되는 암호문 정책 속성중심 암호를 활용한 블록체인 기반 전자의무기록 공유 프레임워크★

백 승 수*

요 약

개인 의료정보는 개인의 존엄성과 가치를 소중히 여기는 개인정보의 한 부분으로서, 만약 불법적인 유출이 되었을 때 한 개인에게 심각한 사회적 편견과 불이익이 돌아올 수 있다. 또한, 그 의료정보는 쓰임새가 많아 그 가치가 상대적으로 높아 내, 외부적인 위협이 지속되고 있는 것이 현실이다. 이에 본 논문에서는 암호문 정책 속성중심 프락시 재암호 기법을 사용하여 블록체인 기반 환자 프라이버시가 보장되는 의료정보공유 프레임워크를 제안한다. 제안하는 프레임워크는 먼저 블록체인을 사용하여 의무기록의 무결성과 투명성을 보장하고, 스텔스 주소를 사용하여 의사-환자의 연계불가성을 제안한다. 또한 암호문 기반 속성중심 암호를 이용하여 세밀한 접근제어가 가능하고, 환자 미동의 및 응급 상황에서의 정보공유가 가능하다.

Blockchain-based Electronic Medical Record Sharing FrameworkUsing Ciphertext Policy Attribute-Based Cryptography for patient's anonymity

Baek Seungsoo*

ABSTRACT

Medical record is part of the personal information that values the dignity and value of an individual, and can lead to serious social prejudice and disadvantage to an individual when it is breached illegally. In addition, the medical record has been highly threatened because its value is relatively high, and external threats are continuing. In this paper, we propose a medical record sharing framework that guarantees patient's privacy based on blockchain using ciphertext policy-based attribute based proxy re-encryption scheme. The proposed framework first uses the blockchain technology to ensure the integrity and transparency of medical records, and uses the stealth address to build the unlinkability between physician and patient. Besides, the ciphertext policy attribute-based proxy re-encryption scheme is used to enable fine-grained access control, and it is possible to share information in emergency situations without patient's agreement.

Key words : Electric Medical Record, Blockchain, Ciphertext-policy Attribute based Proxy Re-encryption

접수일(2018년 11월 15일), 수정일(1차: 2019년 1월 3일), 게재확정일(2019년 3월 29일)

* 고려대학교 정보보호대학원 정보보호학과

★ 이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2017-0-00184, 자기학습형 사이버 면역 기술 개발)

1. 서 론

현재의 보건 의료 분야는 병원 중심에서 환자 중심 및 근거기반 환경으로 급속도로변하고 있으며, 이러한 변화의 기반에는 ICT(정보통신기술)의 발전과 최신 의료 산업 관련 기술이 접목되어 그 원동력이 되고 있다. 이에 따라 보건 의료 기관에서 생성되는 모든 기록을 생성, 이용, 관리하는 방식에서도 많은 변화를 이루고 있는데 가장 대표적인 것이 전자의무기록(Electronic Medical Record, 이하 EMR)이다.

하지만, 이러한 전자의무기록 등 의료정보는 가장 민감한 의료정보이기 때문에 해커들에게 좋은 먹잇감이 되고 있다. 최근 미디어 보도로는 해커들이 개인정보를 암거래하는 시장에서 신용카드 등 금융정보보다 개인 의료정보의 가치를 더 높게 평가하고 있다[1]. 이렇게 환자의 신체적 특징 등 사생활의 유출이 발생하면, 직접적인 불이익을 초래할 수 있다. 예를 들면, 질병이 있던 환자의 회사 면접이나, 보험 혜택, 금융기관 대출 관련 등 인사상의 불이익이 있을 수 있고, 또한, 성 관련 진료나 정신 관련 진료 기록이 유출된다면 타인들이 해당 개인에 대해서 사회적 선입견을 품을 수 있다. 그러므로 개인 의료정보는 사람이 가진 고유한 기본권의 하나로써 충분한 보호를 받지 않으면 안된다.

현재 전자의무기록의 사용은 많은 문제점을 내포하고 있다. 첫째, 환자는 자신의 의무기록관리에 대한 권한이 없어 의료 기관 내 의무기록 조작 가능성이 존재한다. 각 의료 기관의 진료 기록 조작에 대해서는 의료인과 의료 기관의 양심에만 맡길 뿐 별 대책이 없다. 물론 의무기록과 관련해서 의료법 등 각종 규제가 있기는 하지만, 이러한 법 규정에도 불구하고 의료사고가 난 현장에서 의료인이나 병원 관계자가 환자가 호소한 중요한 임상 증상을 임의로 삭제한 경우 환자나 보호자 측이 확인할 방법이 없다. 둘째, 의무기록 공유 시 환자 프라이버시가 보장되지 않는다. 의무기록은 기본적으로 두 가지 목적으로 활용이 된다. 먼저, 진료 예약, 진단, 검사 등 환자의 치료를 목적으로 활용이 되며, 의료 기관 간 공동 연구, 홍보, 환자 교육 등 부가적인 목적으로도 사용할 수 있다. 이때, 환자 개별 동의 또는 의무기록의 익명화는 필수적이다. 하지만, 현재 의무기록의 익명성 관리를 이해 K-Anonymity 등 비식별 기술을 이용하고 있기는 하지만, 쉽게 유추할 수 있어서 신원확인이 가능하다. 셋째, 응급상황이나 미동의 상황에서 공공의 이익을 위해 환자 의무기록의 공유가 제한된다. 환자 의무기록 공유에 있어서 사전에 환자에게 동의를 받는 것은 필수적이다. 하지만, 각종 사고 등 환자가 의식 불명 상태가 될 때 해당 환자의 의무기록을 공유하는 것은 쉬운 일이 아니다. 그렇다고 해서 미리 사고날 것을 가정하여 자신의 의무기록을 열람토록 사전에 동의하는 것은 너무 위험한 일이다. 그러므로 응급상황이 발생하면 환자의 의무기록은 반드시 환자가 신뢰하는 인원에 의해 통제되고 관리된 상황에서 공유되어야 하며, 사후 환자는 열람 기록에 관해 확인할 수 있어야 한다.

그러므로, 본 논문에서 우리는 암호문 정책 속성 중심의 블록체인 기반 의무기록공유 체계를 제안한다. 먼저 우리는 블록체인 기반의 의료정보 시스템의 가져야할 요구사항을 도출하였으며, 이를 기반으로 환자의 익명성과 의사, 환자 간 연계 불가성을 지원하기 위해서 신원 증명용 주소와 별개로 스텔스 주소[2]를 사용하였다. 또한, 의료정보 공유 시 구체적인 접근제어를 하기 위해서 암호문 정책 속성중심 프락시 재암호 기법(Ciphertext-policy Attribute Proxy Re-encryption, 이하 CP-ABPRE)을 사용하여 의무기록 관리를 위한 하이브리드 암호체계를 구축하였다.

본 논문의 순서는 다음과 같다. 2장에서는 제안하는 프레임워크의 기초가 되는 관련 연구 및 제한사항을 언급한다. 또한, 블록체인 기반의 의무기록관리를 위한 보안 요구사항을 도출한다. 3장에서는 암호문 정책기반 속성 중심 암호를 활용한 블록체인 기반 전자의무기록 공유 프레임워크를 제안하고, 4장에서는 2장에서 도출된 보안요구사항에서, 우리가 제안하고 있는 프레임워크가 얼마나 충족하는지 보안성 평가를 하고, 5장에서 결론을 짓는다.

2. 관련 연구

2.1 블록체인

블록체인(Blockchain)[4]은 Peer-to-Peer방식을 기반으로 관리하고자 하는 데이터를 블록(Block)이라는 분산 데이터베이스에 저장하고, 이를 각 블록들 간

에 체인이 형성되어 있어서 누구도 임의로 수정할 수 없고, 누구나 변경의 결과를 열람할 수 있는 분산 컴퓨팅 기반의 데이터 위변조 방지 기술이다. 블록체인의 모든 트랜잭션은 네트워크의 모든 당사자가 있는 분산 원장에 저장된다. 블록체인 기술은 신뢰할 수 없는 트랜잭션을 도입하는 신뢰되는 제 3자 없이 분산 시스템을 구현한다. 이 때, 해당 트랜젝션의 소유권 및 무결성은 신뢰기관이 아닌 암호학적 기술을 통해서 입증된다. 그러므로, 블록체인은 분권화, 불변성, 그리고 비신뢰환경에서의 합의 과정을 통해 데이터의 무결성 및 투명성을 보장한다.

2.2 암호문 정책 속성중심 프락시 재암호 기법(Ciphertext-policy Attribute Proxy Re-encryption)[3]

Cipertext-policy Attribute-based Proxy Re-encryption(이하 CP-ABPRE)는 기존 암호문 정책 중심 암호와 프락시 재암호 기법[5]의 개념을 합친 것으로서, 프락시를 이용하여 동일한 평문으로 생성된 특정 접근 정책기반 암호문을 다른 정책기반 암호문으로 변경할 수 있다. 이는 변화하는 접근 정책에 유동적인 암호문을 재생성할 수 있는 장점이 있다.

먼저 속성기반 암호화(attributed-based encryption)는 복호화 키와 암호화된 데이터에 할당된 속성 또는 접근 정책을 바탕으로 암호화된 데이터에 대한 접근제어 메커니즘을 제공하여 주는 기술이다. 기존 공개키 기반 암호체계에서는 사용자가 시스템을 이용하기 위해서 인증 서버에 사용자 인증을 요구하는 한편, 속성기반 암호에서는 데이터 생성자가 서버에 의존하지 않고 접근제어 정책을 결정할 수 있으며, 속성별 접근제어 규칙을 AND, OR, NOT 등 매우 풍부하게 표현할 수 있다. 게다가, 암호문 정책 속성기반 암호화(CP-ABE)인 경우에는 암호화된 데이터와 접근 트리를 함께 둠으로써 여러 사용자가 속성만 맞는다면 쉽게 접근할 수 있게 된다. 또한, 데이터의 소유자는 제안하는 속성에 따라 접근 정책을 만들 수 있으며, 각 사용자들은 자신의 비밀키만 소유하면 된다.

본 논문에서는 Liang et al[3]가 제안한 CP-ABPRE를 사용한다. CP-ABPRE 는 기존 암호문 정책 속성기반 암호화 방법과 기존 암호문을 복호화하지 않고 변환하여 사용할 수 있는 프락시 재암호화(Proxy Re-Encryption)[5]를 결합한 것이다. 기존의 CP-ABPRE [8, 9]는 안전성이 선택된 평문 공격(Chosen-Plaintext Attack)에만 보장되었으며, 또한 AND 조건만이 가능한 접근제어 형태의 암호문을 생성하였다.

2.3 기존 블록체인 기반 의무기록 공유의 한계

많은 산업체와 학계에서는 의무기록 사용의 한계를 극복하고자 의무기록을 블록체인에 저장해 활용하는 노력을 해왔다. 본 논문에서는 다음의 대표적인 세 블록체인 기반의 의무기록 공유체계를 소개하고 그 문제점을 확인하다.

먼저, Azaria at al[8]은 Medrec 이라는 이더리움 기반의 의무기록 공유 프레임워크를 제안하였다. Medrec은 의무기록은 의료기관의 데이터베이스에 저장하고, 의무기록에 대한 해시값을 블록체인에 저장시킨다. 하지만, Medrec에서는 의무기록을 의료기관 데이터베이스에 저장함에 있어서 암호화에 대한 언급이 없어 비인가자인 의료기관 데이터베이스 관리자에 의무기록 노출이 우려된다. 또한, 참가자별 고정 ID의 사용은 참가자의 익명성을 보존하기 쉽지 않다. 그러므로, 고정된 주소의 재사용은 환자의 익명성을 지키는 데 한계가 있다.

둘째, 영국의 메디컬체인(Medicalchain)[10]이 있다. 메디컬체인은 하이퍼렛저 기반의 의무기록 공유 플랫폼을 제안하였다. 메디컬체인 역시, 사용자 신원은 유일한 UUID를 사용한다. 각 사용자가 유일한 UUID를 사용하게 되면 Medrec에서와 같이 환자의 신원이 드러나게 되는 동일한 문제가 발생한다. 또한, 메디컬체인 역시 네트워크상에서 익명성을 보장하는 메커니즘을 사용하지 않아, 만약 네트워크 관리자가 트랜잭션 발생시와 의무기록 송수신에 대한 IP 주소를 추적한다면 사용자의 신원 추정이 가능하다.

셋째, 한국의 메디블록(Mediblock)[11]이 있다. 메디블록은 QTUM 기반의 의무기록공유 플랫폼이다. 메디블록 역시, 사용자 ID는 서비스 이용마다 지갑주소를 구현하는 것은 경제적이지 않아서 유일한 ID를 사용한다고 주장한다(personnal communication, 5 June, 2018).

위와 같은 주소의 재사용은 Medrec이나 메디컬체인과 같은 이유로 환자 익명성 노출 문제가 발생한

다. 그리고, 네트워크상에서 익명성에 대한 문제도 언급하지 않아서 환자의 익명성 보장이 쉽지 않다. 또한, 응급상황이 발생했을 경우 혈액형 등 간단한 환자의 의료정보만 공유하고, 결국에는 필요한 구체적인 정보가 있을 경우라도 환자가 인증해 주어야만 공유할 수 있다. 그러므로, 안전한 블록체인 기반의 의무기록 공유 프레임워크는 트랜잭션마다 사용자가 가변적인 주소를 사용하여 환자의 익명성을 보장해야 하며, Tor 등 익명성을 보장하는 네트워크를 사용하여 응용단 뿐 아니라 통신상에서도 사용자 익명성을 보장해야 한다. 또한, 응급상황 또는 환자 미동의 상황에서도 암호화된 환자 의무기록에 대한 공유는 필수적이다.

2.4 의무기록 공유체계의 보안요구 사항

본 논문에서는 환자의 의무기록공유에 있어서 다음과 같이 보안 요구사항을 도출한다.

1. 의무기록 암호화 : 해커 및 데이터베이스 관리자를 통해서 불법적인 도청공격이 가능하므로, 반드시 의무기록은 암호화해서 저장되어야 한다.
2. 사용자 신원인증 : 사이비 진료 등 비인가자에 의한 의료행위 및 의무기록 공유를 방지하기 위해서 각 개체의 신원은 확인되어야 한다.
3. 의무기록의 무결성 입증 : 저장, 공유된 의무기록은 불법적인 변경이 없었음이 확인되어야 하며, 시스템 내 누구나 확인 가능해야 한다.
4. 환자의 익명성(Anonymity) 보장 및 연계불가성(Unlinkability)제공 : 저장되는 의무기록은 인가자를 제외하고는 누구의 것인지 확인 불가능해야 한다. 또한, 한 환자로부터 생성된 여러 의무기록이 한 환자 것임이 알려지면 안 된다. 그러므로, 다른 사용자들이 의무기록 간의 연계를 할 수 없어야 한다.
5. 책임 추적성 제공 : 환자의 의무기록을 생성, 저장, 공유, 폐기에 대한 일련의 행위 등에 대해서, 이 행위를 행한 인원과 특정 시간에 발생한 행위는 파악되어야 한다.
6. 공모에 의한 공격 예방 : 비인가자들끼리 공모에 의해서 환자의무기록을 열람하던지, 송, 수신 내역 등 환자가 진료를 받았다는 사실조차 알 수 없어야 한다.
7. 응급상황 및 환자의무기록 공유 미동의 상황에서의 공유 : 응급상황이 발생하였을 때, 환자에게 동의를 받지 않았다 하더라도 최소한의 권한으로 제 3자와 의무기록공유가 가능해야 한다.

<표 4> 제안하는 의무기록 블록체인 접근제어규칙

역할	환자	주치의	제3자	감독기관	검증자
생산	×	○	×	×	×
확인	○	○	△	△	×
접근제어	○	△	×	×	×
공유	○	△	×	×	×
삭제	×	×	×	×	×
※ 범례 : ○(항시가능), △(환자동의 후 가능),×(불가)					

3. 제안하는 암호문 정책기반 속성 중심 암호를 활용한 블록체인 기반 전자의무기록 공유 프레임워크

3.1 의무기록 접근제어 구조

본 논문에서 사용되는 블록체인은 프라이빗 블록체인이다. 프라이빗 블록체인은 감독기관을 중심으로 읽기, 쓰기, 합의 과정에서 참여할 수 있는 인원이 미리 지정되어 있으며, 필요에 따라 주체가 새로 추가되거나 삭제될 수 있다. <표 3>은 의무기록 블록체인에서 사용되는 각 주체별 접근제어 규칙 언급한다.

3.2 제안하는 블록체인 트랜잭션 구조

본 트랜잭션을 통해서 환자 진료 후 생성된 환자의 무기록에 대한 저장, 공유 및 폐기에 대한 모든 활동 상황이 블록체인에 입력이 된다. 트랜잭션은 의무기록 검증자에게 검증을 받고 <표 4>의 트랜잭션 형태로 블록에 저장된다.

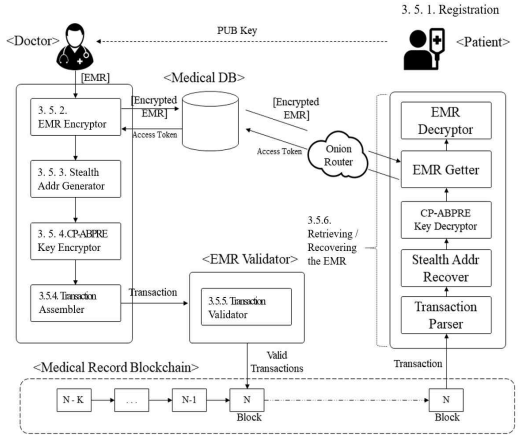
<표 5> 제안하는 의무기록 블록체인 트랜잭션 구조

Index	내용
TxID	트랜잭션의 일련번호.
TxHash	본 트랜잭션에 대한 전체 비트열을 입력하여 해시 함수를 통해 산출된 해시값.
Timestamp	트랜잭션 시점의 기록
TxAction	본 트랜잭션에 대한 활동상태를 기록
From	주체의 주소 값
To	공유할 객체의 주소 값 (Stealth Address 사용)
Public Parameter	스텔스주소를 조합하기 위한 송신자가 보내는 공공변수
Plain Record Digest	실제 환자의무기록이 해시함수를 통해 산출된 고정길이의 비트열.
Cipher Record Digest	암호화된 환자의무기록이 해시함수를 통해 산출된 고정길이 해시값.
Access Token	의무기록을 암호화할 때 쓰인 Key값을 CP-ABPRE를 통해 암호화한 값.
Access URL	의무기록 데이터베이스의 주소

3.3 제안하는 의무기록 공유 프레임워크

본 논문에서는 환자의 익명성이 보장되는 블록체인 기반의 의무기록 공유 프레임워크를 제안한다. 제안하는 프레임워크는 다음의 세 가지로 나눌 수 있다. 먼저 환자 의무기록의 투명성과 무결성을 보장하기 위해서 프라이빗 블록체인 네트워크를 사용한다. 블록체인은 모든 트랜잭션이 순서에 의해 기록되며 서로 연결되어 있다. 이 때문에 블록에 기록된 내용은 수정이 힘들고 추적이 가능하다.

둘째로, 스텔스 주소를 사용하여 블록체인 상에서 환자의 익명성과 연계 불가성을 보장한다. 암호화폐인 모네로[2]에서 사용되는 스텔스 주소는 수신자의 익명성 및 연계 불가성을 보장한다. 발신자는 수신자가 제공하는 공개키 값을 갖고 일회용 주소로 변환하며, 오로지 수신자만이 특정 트랜잭션이 자신과 연관 있음을 확인 가능하다.



(그림 1) 제안하는 의무기록공유 프레임워크

셋째로, 세밀한 접근제어 및 암호화된 의무기록의 접근권한을 이전하기 위해서 CP-ABPRE[3]를 사용한다. CP-ABPRE는 먼저 암호문 정책 속성기반 암호화 기법의 속성을 그대로 따르게 되는데 환자는 세밀한 접근제어 구조를 통해서 의무기록 열람자 통제가 가능하고, 의무기록 열람자는 자신의 비밀키만 소유하면 된다는 장점이 있다. 그리고, CP-ABPRE는 프락시 재암호화를 지원한다. 여기에서 프락시는 암호문을 변환하기 위한 키를 사용하여 기존의 암호문을 복호화 없이 변환하기 때문에 평문이나 A의 비밀키를 알지 못한다. 따라서 암호화된 데이터의 안전성을 보장하면서 열람 권한이 위임할 수 있다.

위에서 제안한 블록체인 구조를 바탕으로 환자의 프라이버시를 보장하면서 환자의무기록을 안전하게 공유하는 프레임워크는 (그림 1) 과 같다.

3.5.1 환경설정 및 사용자 등록

먼저, 감독기관은 의무기록 블록체인 시스템을 구성하기 위해서 사용자들에게 제공할 변수들을 <표 5> 같이 구성한다. 시스템 구성이 끝난 후 환자, 의사 응급치료사 등 블록체인 사용자는 자신의 신원을 증명하고, 의무기록을 암호저장 및 공유하기 위해서 다음과 같은 절차를 밟는다.

1. 신원확인 : 먼저 사용자는 감독기관에 자신의 신원을 증명하기 위한 서류를 제출한다.
2. 신원 확인용 키 발급 : 감독기관은 서류를 접수하

<표 6> CP-ABPRE Setup 단계

CP-ABPRE Setup
Input : security parameter
Output : public parameter pp, master key msk
1. choose random value $a, \alpha \in Z_p^*$ 2. setup TCR hash functions $_1$: $0,1\}^{2k}$ Z_p^*, $H_2 : G$ $\{0,1\}^{2k}$ $H_3, H_4 : \{0,1\}^*$ G, $H_5 : \{0,1\}^k$ Z_p^* $H_6 : \{0,1\}^*$ G 3. public parameter $pp = (p, g, G_T, G, g_1, g^\alpha, e(g,g)^\alpha, H_1, ..., H_6$ 4. master key g^α

고, 의료행위 신원 확인을 위한 공개키 쌍을 발급한다. 예를 들면, 환자 A 인 경우, 감독기관은 환자용 임의의 개인 키 $PR_A \in \{1, ..., p-2\}$을 찾아 공개키 $PU_A = PR_A$ G를 계산해 낸다. 이 때, 감독기관은 간단히 사용자가 자신의 신원을 드러낼 수 있는 가명(pseudonym) 사용자 주소를 아래 <수식 1>과 같이 제공한다.

$$Addr_{id} = \mathrm{BASE}_{58}(\mathrm{RIPEMD160}(SHA256(PU_{id}))) \quad (1)$$

3. 의무기록용 속성 개인 키 발급 : 사용자는 자신의 신원 속성에 대해서 속성 개인 키를 발급받는다. 속성 개인키는 의무기록 블록체인 상의 키 공유를 위해 필요하다. 먼저 감독기관은 <표 5>에서 산출한 마스터키(msk)와 속성 집합 S 를 갖고 사용자의 속성 키 sk_S 를 <수식 2>와 같이 만든다. 예를 들면, 의사 B 가 자신을 드러낼 수 있는 속성이 '심장외과, 의사B, 성모병원, 자격기간:20200909'라면, 각각 속성 키를 구하는 속성집합 S의 원소가 될 수 있다.

$$K = g^\alpha \quad ^t \quad g^\alpha, L = g^t, \quad _x \in S \; K_x = H_3(x)^t \quad (2)$$

3.5.2 환자 의무기록 생성(EMR Encryptor)

다음은 환자 의무기록 생성 및 데이터베이스 저장 단계이다. 본 논문에서는 환자 A 와 주치의 B 사이에 환자 의무기록을 생성 저장하는 것을 전제로 한다. 우선 환자 A는 자신의 신원을 검증하기 위해서 주치의 B에게 감독기관으로부터 부여받은 주소 값 $Addr_A$를 제시한다. 주치의 B는 진료받을 환자 A가 맞는지

<표 7> 접근제어 키 암호화

Key Encryptor
Input : Key Key_{EMR}, Access Rule (M, ρ)
Output : Ciphered Key $CK_{(M,\rho)} = (A_1, A_2, A_3, (B_1, C_1), ..., (B_l, C_l), (M, \rho), D)$
1. Random choose $\beta \in \{0,1\}^k$ 2. Set $H_1(Key_{EMR}, \beta)$ 3. Set a random vector $v = (s, y_2, ..., y_n)$ such that $y_2, ..., y_n \in Z_p^*$ 4. For $i = 1$ to l, Set $\lambda_i = v$ M_i such that M_i is a i th row vector. 5. Random choose $r_1, ..., r_l \in Z_p^*$ 6. Set $A_1 = Key_{EMR}$ β $H_2(e(g,g)^\alpha \quad ^s)$, $A_2 = g^s$, $A_3 = g_1^s$, $B_1 = (g^a)^\lambda$ $H_3(\rho(1))^{-r_1}, C_1 = g^{r_1}, ...$ $B_l = (g^a)^{\lambda_l}$ $H_3(\rho(l))^{-r_1}, C_l = g^{r_l}$ such that $\rho(i)$ is i th attribute of matrix (M, ρ) 7. Set $D = H_4(A_1, A_3, (B_1, C_1), ..., (B_l, C_l), (M, \rho))^s$

확인하기 위해서, 감독기관에 공개된 A의 공개키 PU_A를 받아서 아래 <수식 3>과 같이 산출하여 비교한다.

$$Addr_A \stackrel{?}{=} \mathrm{BASE}_{58}(\mathrm{RIPEMD160}(SHA256(PU_A))) \quad (3)$$

주치의 B는 대면한 환자의 신원을 확인하고 진료를 시작한다. 진료 후, 주치의 B는 환자 A의 의무기록 내용 M_A를 생성하고 생성자 및 무결성을 입증하기 위해서 <수식 4>와 같이 전자서명을 하여 의무기

록 MR 를 완성한다.

$$EMR_A \quad Addr_A \quad Addr_B \quad t \quad M_A \quad Sig(Addr_A \quad Addr_B \quad t \quad M_A, PR_B) \tag{4}$$

주치의 B는 $0,1\} \in G_T$ 를 만족하는 임의의 정수 Key_{EMR}을 선택하여, EMR_A를 만들어 <수식 5>와 같이 암호화하며, 암호화된 의무기록 CT_{EMR}을 만들어 낸다. 여기서 원활한 암호화를 위해 대칭키 암호체계인 AES를 활용한다.

$$CT_{EMR} = AES_{enc}(EMR_A, Key_{EMR}) \tag{5}$$

3.5.3 스텔스 주소 및 접근제어 구조 생성(Stealth Addr Generator)

다음 주치의 B는 환자 A의 의무기록을 공유하고, 환자-의사간 연계성을 없애기 위해서 환자를 위한 스텔스 주소[2]를 주소를 <수식 6>과 같이 계산한다.

$$SA_A = (H(r \quad PU_A) \bmod p) \quad G + S_A \tag{6}$$

주치의 B는 자신의 신원 주소와 위 <수식 6>에서 계산한 스텔스 주소를 포함하여 환자 A에 대한 접근제어 규칙을 <수식 7>과 같이 만들어 낼 수 있다.

$$(M, \rho) = (Addr_A \text{ and } SA_A) \; OR \; Addr_B \tag{7}$$

(, M은 $l \times m$ 매트릭스이며, ρ는 M과 연계된 함수임.)

3.5.4 접근제어 키 암호화 및 데이터베이스 저장(CP-ABPRE Key Encryptor & Transaction Assembler)

주치의 B는 암호화된 의무기록 CT_{EMR}을 복호화 할 수 있는 Key_{EMR}에 대해 Liang et al[3]. 의 CP-ABPRE 스킴을 사용하여 접근제어 키 Key_{EMR}를 <표 6>와 같이 암호화 한다. 주치의 B는 암호화된 의무기록 CT_{EMR}의 무결성을 보장을 위해, $H(CT_{EMR})$같이 해시 값을 추출해낸다. 다음 주치의 B는 원격으로 접속할 수 있는 의료기관 데이터베이스에 CT_{EMR}과 $H(CT_{EMR})$을 저장한다. 의료기관 데이터베이스는 CT_{EMR}가 잘 저장되어 있음을 확인하고, 접근할 수 있는 임의의 접속 URL을 반환한다. 이때, 데이터베이스 관리자는 주치의 B 가 의무기록을 입력했다는 사실은 알지만, 암호화되어 있으므로 누구의 의무기록인지 확인 불가능하다. 이 후, 주치의 B는 트랜잭션를 아래와 같이 생성하여 의무기록 검증자에게 전달한다.

3.5.5 트랜잭션 검증 및 블록 생성(Transaction Validator)

본 논문은 프라이빗 블록체인 형태를 그대로 사용하므로 거래 장부를 분산한다는 점은 같으나, 작업증명과 채굴과정을 생략하고 대신 감독기관이라는 관리주체가 거래의 승인 및 블록 생성 권한을 보유한다. 그러므로, 감독기관으로부터 허가받은 의료기록 검증자는 의료기관으로부터 트랜잭션을 수신하게 트랜잭션 그 자체의 무결성을 해시값으로 검증한다. 위 과정이 완료되면 의무기록 검증자는 다시 한번 트랜잭션의 블록 해시 값을 구한다. 특정 시간이 지나 트랜잭션 풀(pool)이 차면, 블록에 삽입한다.

3.5.6 데이터 검색 및 복구

이번 단계에서는 환자 A가 의무기록 블록체인에서 자신과 관련된 블록을 찾아, 의료 데이터베이스로부터 의무기록을 얻고, 복호화 하는 과정을 설명한다. 먼저 환자 A는 블록체인 상의 자산과 연계된 스텔스 주소를 추출하기 위해서 <수식 10>에 맞는 주소 값을 계산하여 찾아낸다. 이때, 환자는 트랜잭션 상의 공공변수(public parameter) 값인 R과 To 항목의 주소를 찾아 계산한다.

$$SA_A = (H(R \quad PR_A) \bmod p) \quad G + S_A \tag{10}$$

해당하는 블록의 트랜잭션을 찾은 환자 A는 직접 해당 의무기록이 있는 데이터베이스에 접속을 시도한다. 이 때, 접속하기 전에 자신의 네트워크 주소가 노출되지 않게 하도록 Tor 등 익명성을 보장하는 네트워크를 사용하여 접속한다. 왜냐하면, 통신 구간에서 환자의 신원을 노출하지 않기 위함이다. 다음, 환자 A는 해당 URL에 접속하여 데이터베이스에 암호화된 의무기록을 요청한다. 의료 데이터베이스는 저장되어 있던 CT_{EMR}을 반환하고, 환자 A는 <표 7> 와 같이 복호화 한다.

<표 8> 환자 A의 의무기록 복원

Retrieving and Recovering the EMR
Input : a private key k', encrypted key $K_{(\ ,\rho)}$, encrypted record CT_{EMR}
Output : EMR of Patient A EMR_A
1. parse the encrypted key $CK_{(M,\rho)} = (A_1, A_2, A_3, (B_1, C_1), ..., (B_l, C_l), (M, \rho), D)$ 2. Compute $e(A_2, K) / (\prod_{i \in I} (e(B_i, L) \quad e(C_i, K_{\rho(i)}))^{w}$ $= \frac{e(g, g^{a \quad t} \quad g^{\alpha})}{e(g, g^{a \quad t})^{\sum_{i \in} \lambda_i \quad w_i}} = e(g^s, g^{\alpha})$ 3. Then $H_2(e(g^s, g^{\alpha})) \quad A_1$ $= H_2(e(g^s, g^{\alpha})) \quad (Key_{EMR} \quad \beta)$ $H_2(e(g^s, g^{\alpha}))$ $= Key_{EMR} \quad \beta$ 4. Extract Key_{EMR} 5. Decrypt EMR_A $= S_{dec}(CT_{EMR}, Key_{EMR})$ 6. Check the integrity of EMR_A

3.5.6 환자 의무기록 긴급 공유

환자가 사고로 인해 응급상황이거나 혼수상태 였을 때, 환자의 의무기록을 공유해야 하는데 쉽지 않을 경우가 있다. 이 때, 응급치료사는 응급센터에 요청하여 환자의 의무기록을 받아볼 수 있어야 한다. (그림 2)는 응급상황 시 의무기록을 공유하는 프레임워크를 설명한 것이며 세부적인 내용은 다음과 같다.

- 응급센터의 환자의무기록 요청: 응급치료사는 응급센터에 해당 인원에 대한 환자의무기록을 요청하며, 응급센터는 수소문하여 환자에 대한 의무기록을 생성한 주치의 B를 찾아낸다. 주치의 B는 해당하는 트랜잭션 번호를 알려주며, 알려주었다는 사실을 블록체인에 기록한다. 트랜잭션 번호를 안 응급센터는 위 데이터 검색 방법과 같이 해당하는 데이터베이스에 접근하여 환자의 의무기록 CT_{EMR}을 얻는다. 이 때, 주치의 B는 기존 환자의 의료기록을 응급센터와 공유한다는 트랜잭션을 남긴다.

<표 9> 응급용 키 재발행

Private Key Re-keying
Input : a private key sk_s, attribute set S, new access structure (M', ρ')
Output : new private key $sk_S{}^{w}$
1. Choose random $\beta, \delta \in \{0,1\}^k$ 2. Set $s' = H_1(\delta, \beta')$ 3. Set a random vector $v' = (s', y_2', ..., y_n') \in Z_P^*$ 4. For $i = 1$ to l': Set $\lambda_i' = v' \quad M_i'$ 5. Choose $r_1', ..., r_l' \in Z_P^*$ 6. Compute $A_1' = (\delta \quad \beta) \quad H_2(e(g,g)^{\alpha \quad s'}) A_2' = g^{s'}$, $B_1' = (g^a)^{\lambda_1'} \quad H_3(\rho(1)')^{-r_1'}, C_1' = g^{r_1'}, ...$ $B_l' = (g^a)^{\lambda_l'} \quad H_3(\rho(l')')^{-r_l'}, C_l' = g^{r_l'}$, $D' = H_6(A_1', A_2', (B_1', C_1'), ..., (B_l', C_l'), S, (M', \rho'))^{S'}$ 7. Assemble $C_{(M', \rho')}$ $= ((M', \rho'), A'_1, A'_2, (B'_1, C'_1), ..., (B'_l, C'_l), D')$ 8. Choose random $\theta = Z_P^*$ 9. Set $rk_1 = K^{H_5(\delta)} \quad g_1^{\theta}$, $rk_2 = g^{\theta}$, $rk_3 = L^{H_5(\delta)}$, $rk_4 = C_{(M', \rho')}$, $R_x = K_x^{H_5(\delta)}$ 10. Output $sk_s{}^{w} = (S, rk_1, rk_2, rk_3, rk_4, R_x)$

- 주치의 B의 재암호화를 위한 키 재발행: 요청을 받은 주치의 B는 응급치료사가 기존 의무기록을 복호화할 수 있도록 새로운 접근제어 구조 (M', ρ')를 만들어 낸다. 그리고, 해당 응급치료

사가 의무기록을 열 수 있도록 <표 8> 과 같이 응급용으로 사용할 키 k^{w}를 재발행하여 응급 센터에 전달한다.

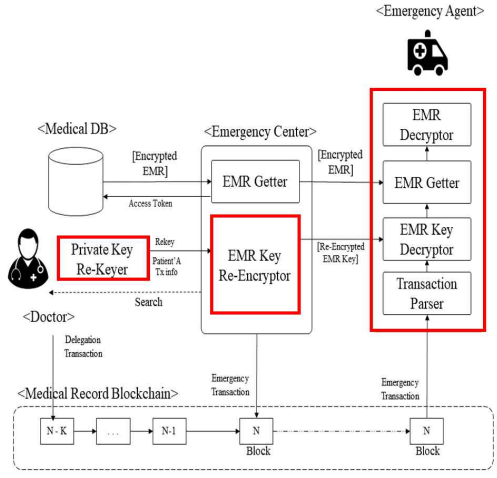
<표 10> 응급용 의무기록 재암호화

EMR Key Re-encrypting
Input : Re-key $sk_S{}^{w}$, Encrypted Key $K_{(M,\rho)}$
Output : Re-encrypted Key $CK'_{(M',\rho')}{}^{w}$
1. Verify if $sk_S{}^{w}$ includes S : $e(A'_2, H_6(A'_1, A'_2, (B'_1, C'_1), \ldots, (B'_l, C'_l), S, (M', \rho'))^{s'}) = ?\, e(g, D')$ 2. Compute $A_4 = \prod_{i \in I} (e(B_i, rk_3) \quad e(C_i, R_{\rho(i)}))^{w}$ $e(A_2, rk_1) \quad e(A_3, rk_2)$ 3. Output $CK'_{(M',\rho')}{}^{w} = (S, (M, \rho), A_1, A_3, (B_1, C_1), \ldots, (B_l, C_l), D, A_4, rk_4)$

<표 10> 응급용 의무기록 복구

Recovering the EMR with Re-key
Input : Emergency agent's private key sk'_S, Re-Encrypted Key $CK'_{(M',\rho')}{}^{w}$, Encrypted Medical Record CT_{EMR}
Output : Patient A's EMR EMR_A
1. Compute $Z' = \prod_{i \in I} (e(B'_i, L') \quad e(C'_i, K(\rho(i)')'))^{w}$ $e(A'_2, K')$ 2. Compute $H_2(A_4^{\frac{1}{H_5(\delta)}}) \quad A_1$ $= H_2(e(g,g)^{\alpha \quad s \quad H_5(\delta)})^{\frac{1}{H_5(\delta)}} \quad H_2(e(g, g$ $Key_{EMR} \quad \beta$ 3. Extract Key_{EMR} 4. Decrypt $EMR_A = S_{dec}(CT_{EMR}, Key_{EMR})$

- 기존 암호화된 의무기록 키의 재암호화: 암호화된 의무기록 CT_{EMR}을 수신한 응급센터는 주치의 B로부터 받은 재발행한 응급용 키를 사용하여 <표 9>와 같이 암호화된 의무기록을 복호화 할 수 있는 키인 $CK_{(M,\rho)}$를 재암호화한다. 다음 응급센터는 재암호화된 의무기록 키 $CK'_{(M',\rho')}{}^{w}$를 응급 치료사에게 전달한다. 감독기관은 자신이 응급용으로 재암호화 했다는 사실을 블록체인에 올린다.
- 응급치료사의 재암호화된 의무기록 복호화: 응급치료사는 감독기관으로부터 기존 암호화된 의무기록 CT_{EMR}, 새롭게 암호화된 의무기록 키 $CK'_{(M',\rho')}{}^{w}$와 관련한 블록체인 트랜잭션 번호, 그리고 응급용 키 $sk_S{}^{w}$을 받았다. 다음 응급치료사는 <표 11>을 통해서 암호화된 의무기록을 복호화 한다.



(그림 2) 환자의무기록 긴급공유

4. 보안성 평가

본 장에서는 위에서 제안한 블록체인 기반의 의무기록 프레임워크가 2장에서 언급한 보안 요구사항을 어떻게 충족하는지 알려준다. <표 12>은 제안하는 프레임워크와 기존 블록체인 기반의 의무기록 체계와의

보안 요구사항을 충족하는 가를 비교한 것이다.

<표 11> 제안하는 프레임워크와 기존 체계 비교

구 분	Ours	[8]	[10]	[11]
의무기록 암호화	○	○	○	×
사용자 신원인증	○	○	○	×
의무기록 무결성	○	○	○	○
환자익명성, 연계불가성	○	×	×	×
책임추적성	○	○	○	○
공모공격 방지	○	×	×	×
응급/환자 미동의 상황 공유	○	△	△	×
※ 범례 : ○(항시가능), △(환자동의 후 가능), ×(불가)				

4.1 의무기록 암호화

제안하는 프레임워크는 메디컬체인[10]이나 메디블록[11]과 같이 대칭키 암호 알고리즘을 이용해서 의무기록을 암호화한다. 그리고, 이때 사용된 키를 CP-ABPRE를 통해서 암호화하고 조건에 맞는 수신자가 의무기록을 복구할 수 있도록 한다. 이때, 환자는 자신의 의무기록 접근 조건을 구체화할 수 있으며, 의무기록을 수신하는 사용자는 자신의 속성 개인 키를 이용해서 의무기록을 수신하여 복구할 수 있다.

4.2 사용자 신원인증

제안하는 프레임워크는 허가형 프라이빗 블록체인이기 때문에 감독기관이 발행한 키를 사용해야지만 이용할 수 있다. 신원확인 시 감독기관에 해당 인원의 공개키를 발급받아 주소 값을 매칭시킬 수 있다.

4.3 의무기록 무결성 입증

의무기록의 무결성을 보장하기 위해 의사는 자신이 발행한 의무기록에 대한 해시 값을 블록에 올리고, 수신자는 의료 기관으로부터 수신한 의무기록을 복호화하고 블록에 있는 해시 값과 서로 비교하여 그 무결성을 확인할 수 있다.

4.4 환자의 익명성(Anonymity) 및 연계불가성(Unlinkability) 보장

의무기록은 인가자를 제외하고는 누구의 것인지 확인 불가능하다. 우리는 기본적으로 통신에서 환자의 익명성과 응용단에서 환자의 익명성을 기술하였다. 통신 구간에서는 Tor네트워크 등 겹층 암호화된 라우팅 기술을 사용하여 실제 송, 수신자가 누구인지 네트워크 관리자 및 데이터베이스 관리자가 확인할 수 없도록 하였으며, 응용단에서는 환자와 의사의 연계불가성을 유지하기 위해서 스텔스 주소를 사용하였다. 여기서 의사는 임의의 정수 R을 지속적으로 생성하여, 동일한 환자의 여러 의무기록에 대한 연계성을 없앨 수 있다. 만약, 블록체인 네트워크 상에 존재하는 사용자가 N명이라고 가정할 경우에는, 네트워크 관리자 등 비 인가자는 실제 환자의 의사와의 연계성을 1/N의 확률로 추정해야 한다. 또한 스텔스 주소의 세션 가 지속적으로 변화하기 때문에 비인가자가 해당환자를 추측해 내기가 쉽지 않다. 게다가 블록체인 상에서는 환자의 의무기록 대신 해시 값만 삽입이 되므로 블록만으로 누구의 의무기록에 대한 설명인지 확인할 수 없다. 그러므로 제안하는 프레임워크는 기존 Medrec, 메디컬체인, 메디블록과 달리 환자의 익명성을 보장하며, 환자와 트랜잭션간 연계불가성을 제공한다.

4.5 책임 추적성 제공

네트워크 참여자는 의무기록을 생성, 저장, 공유, 폐기에 대한 모든 내용을 블록체인에 기록함으로써 누가 어떤 행위를 하였는지 알 수 있다. 만약, 환자와 의사 간의 의료 분쟁이 생겼을 때, 환자는 자신의 스텔스 주소를 입증함으로써 해당 의사가 발행한 의무기록이 어떤 것인지 확인할 수 있다.

4.6 공모에 의한 공격 예방

제안하는 프레임워크는 의무기록 생성단계에서 바로 암호화되어 저장이 되므로 데이터베이스 관리자는 누구의 의무기록인지 확인 불가능하다. 또한, 위에서 언급했 듯 제안하는 프레임워크는 환자의 익명성을 보장하고 연계불가성을 제공하기 때문에 네트워크 관리자도 공유하는 의무기록이 누구에게 연결이 되는지

확인 불가능하다. 그러므로 데이터베이스 관리자 및 네트워크 관리자가 얻어지는 정보가 없으므로 서로 공모하는 것이 무의미하다.

4.7 응급 상황 및 환자 의무기록 공유 미동의 상황에서의 공유

본 프레임워크에서는 감독기관 프락시 재암호화 기능을 통해서 응급상황이 발생하였을 때, 환자의 동의를 받지 않았다 하더라도 최소한의 권한으로 제 3자와 의무기록 공유가 가능하다.

5. 결 론

본 논문에서는 블록체인 기반의 환자의 프라이버시가 보장되는 의료정보 공유 프레임워크를 제안하였다. 우리는 먼저 블록체인 기반의 의료정보 시스템의 가져야할 요구사항을 잠재적 위협원과 같이 도출했다. 그리고 이를 기반으로 환자의 익명성과 의사, 환자간 연계 불가성을 지원하기 위해서 신원 증명용 주소와 별개로 스텔스 주소를 사용하였다. 또한, 의료정보 공유 시 구체적인 접근제어를 하기 위해서 CP-ABPRE 암호 알고리즘을 사용하여 의무기록 관리를 위해서 하이브리드 암호체계를 구축하였다. 제안하는 방식은 암호화 키를 접근제어 방식과 결합해 속성이 노출되더라도 다른 접근 권한을 변경할 수 있는 장점이 있다. 또한, 응급상황 및 환자 미동의 상황에서도 감독기관이 암호화된 키를 유지한 채로 응급 수신자에게 알맞게 재암호화함으로써 정보를 공유할 수 있었다.

따라서 본 연구는 블록체인 기반의 분산 환경에서, 환자 의료정보의 기밀성과 무결성을 보장하는 의료정보공유 프레임워크를 제안한 것이다. 하지만, 의료 정보의 저장이 의료 기관에 한정되어 있기 때문에, 가용성에 대한 제한 사항이 존재한다. 향후 연구로는 분산 DB를 활용하여 위 프레임워크에 접목시킨다면, 보다 효율적이고 실용적인 방안이 될 것으로 판단된다.

참고문헌

[1] Humer, Caroline, and Jim Finkle. "Your medical record is worth more to hackers than your credit card." Reuters. com US Edition 24 (2014).

[2] Monero, “How does monero’s privacy work?” https://www.monero.how/how-does-monero-privacy-work (2018.11.11.접속)

[3] Liang, Kaitai, et al. "A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security." Intelligent Networking and Collaborative Systems (INCoS), 2013 5th International Conference on. IEEE, 2013.

[4] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[5] Mambo, Masahiro, and Eiji Okamoto. "Proxy cryptosystems: Delegation of the power to decrypt ciphertexts." IEICE transactions on fundamentals of electronics, Communications and computer sciences 80.1 (1997): 54-63.

[6] Liang, Xiaohui, et al. "Attribute based proxy re-encryption with delegating capabilities." Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. ACM, 2009.

[7] Luo, Song, Jianbin Hu, and Zhong Chen. "Ciphertext policy attribute-based proxy re-encryption." International Conference on Information and Communications Security. Springer, Berlin, Heidelberg, 2010.

[8]Azaria, Asaph, et al. "Medrec: Using blockchain for medical data access and permission management." Open and Big Data (OBD), International Conference on. IEEE, 2016.

[9] Conti, Mauro, et al. "A survey on security and privacy issues of bitcoin." IEEE Communications Surveys & Tutorials (2018).

[10] MedicalChain, “whitepaper v2.0,” https://medicalchain.com/en/ (2018.11.11.접속)

[11] MedicalBlock, “whitepaper v1.0,” https://medicalchain.com/ko/ (2018.11.11.접속)

〔저자소개〕

백 승 수 (Seungsoo Baek)
2002년 3월 육군사관학교 전산학학사
2007년 9월 Naval Postgraduate School 전산학 석사
2018년 9월 고려대학교 정보보호대학원 정보보호학 박사
email : offident79@korea.ac.kr