# 의료 데이터의 무결성과 보안을 위한 사이드 체인 기반 데이터 공유 시스템

오윤재, 허가빈, 도인실

이화여자대학교

angelaoh@ewhain.net, gjrkqls@ewhain.net, isdoh1@ewha.ac.kr

# Side Chain Based Data Sharing System for Integrity and Security of Medical Data

Yoonjae Oh, Gabin Heo, Inshil Doh

Ewha Womans University

요 약

현재 의료 분야에서 IoT 기기가 활발히 사용되면서 환자들의 개인 정보 및 의료 데이터에 대한 보안 문제가 대두되고 있다. 본 연구에서는 IoT와 블록체인을 융합하여 의료 데이터의 무결성과 보완을 유지하면서 신속하게 다른 병원들과 데이터를 공유할 수 있는 시스템을 제안한다. 각 병원은 사이드 체인을 형성하여 부서별로 환자 데이터를 안전하게 관리하고, 메인 노드 간의 메인 체인을 통해 데이터를 빠르고 신속하게 공유한다. 사이드 체인에서 블록 생성 시 리더 노드를 선출함으로써 신뢰도가 보장된 시스템이 마련되며, IoT 기기 대신 부서별 대표 노드를 블록체인 노드로 사용하여 IoT 기기의 부담을 줄였다. 메인 체인에서는 사이드체인 블록을 메타 데이터로 압축하여 트랜잭션을 생성함으로써 오버헤드를 줄이고자 하였다. 제안된 시스템은 의료 데이터의 보안과 무결성을 보장하면서 병원 간 데이터 공유를 통해 효율적인 의료가 가능하도록 한다.

## Ⅰ. 서론

IoT(Internt of Things)는 일상적인 물건이나 기기를 인터넷에 연결하여 상호작용하고 정보를 주고받게 하는 기술로, 사물 간의 효율적인 통신과 정보 수집을 가능케 한다. 현재 IoT 기술은 스마트 홈, 스마트 농장, 에너지 관리 등 여러 분야에서 활용되고 있으며 환자의 건강을 책임지는 의료분야에서도 활발히 사용되고 있다. 의료 분야의 IoT는 의료 기기와 기술이 인터넷을 통해 연결되어 데이터를 공유하는 방식으로 활용되고 있다. 환자 모니터링, 스마트 의료 기기, 전자 의료 기록, 치료 및 개인화된 의료 서비스, 긴급 상황 대응 등에서 활용되어 의료 분야를 혁신하고 있다.

하지만 의료 IoT 기기들이 정보를 주고받는 과정에서 다양한 보안 및 개인 정보 위험이 존재한다. 기기들이 정보를 주고받을 때 환자의 개인 정보 및 의료 데이터가 노출될 수 있고 악의적인 노드가 개입하여 정보를 조작하여 거짓된 개인 정보 및 데이터를 전달할 수 있다[1]. 도용된 개인 정보는 악의적으로 사용될 수 있고 조작된 데이터는 의료기기에 오작동을 일으켜 환자 건강에 치명적인 영향을 끼치게 된다[2]. 따라서 의료 데이터의 보안과 정확성을 위해 블록체인과 IoT를 융합하여 이러한 문제점을 해결하려는 시도들이 이어지고 있다. 하지만 IoT 기기는 한정적인 저장공간과 연산 능력을 가지고 있기 때문에 이러한 점을 고려하여 블록체인과 IoT 기기를 융합해야 한다.

본 연구에서는 병원 단위로 사이드 체인을 구성하여 해당 병원 환자들의 의료 데이터를 부서 단위로 안전하게 관리하고, 병원의 메인 노드들이 메인체인 네트워크를 형성하여 병원 간에 환자 데이터를 안전하고 신속하게 공유할 수 있는 시스템을 제안하고자 한다.

## Ⅱ. 관련 연구

IoT와 블록체인의 융합은 크게 두 가지 방식으로 이루어진다. 첫 번째는 IoT 기기를 블록체인 노드로 사용하는 방법이다. [3]의 연구에서는 이동성이 작고 저장 용량이 상대적으로 큰 일부 기기만 블록체인 노드로 사용하고 PoS를 합의 매커니즘으로 사용하는 방법을 제안하였다. 두 번째는 방법은 자원이 충분한 기기를 IoT 기기를 대신하여 블록체인 노드로 사용하는 것이다. [4]의 연구에서는 IoT 기기들이 클러스터를 형성하여 클러스터마다 용량이 큰 기기를 헤드 노드로 지정하여 헤드 노드들끼리 블록체인 네트워크를 형성하는 방법을 제시하였다.

해당 연구들은 IoT 기기에 블록체인을 적용한 범용적인 방법이기 때문에 데이터의 무결성과 보완성이 중요한 의료 시스템에 적합하지 않다. 본 연구는 이와 같은 의료 데이터의 특성에 초점을 맞추어 IoT 기기와 블록체인을 융합한 의료 데이터 공유 시스템을 제안하고자 한다.

## Ⅲ. 사이드 체인 기반 의료 데이터 공유 시스템

### 1. 시스템 구조 및 블록 구조

본 연구에서는 병원들이 각자 하나의 사이드 체인을 형성한다. 그리고 병원마다 1개의 메인 노드가 존재하여 해당 노드들이 메인 체인을 형성한다.

a. 병원 단위로 배치된 사이드 체인

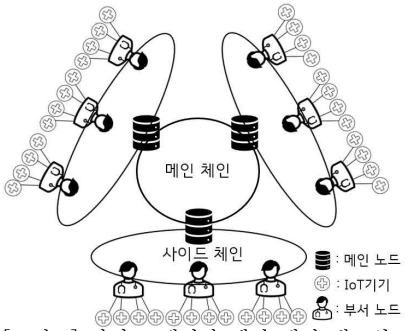
각 병원에는 부서별로(ex. 정형외과, 신경외과, 피부과) 1개의 부서 노드가 존재한다. 각 부서 노드들은 [그림 1]과 같이 자신이 담당하고 있는 부서의 IoT 기기들로부터 환자의 데이터를 전달받는다. 여기서 IoT 기기들은 수집한 데이터를 자신의 부서 노드로 전송하는 역할만 하고 블록체인에는 참여하지 않는다. 부서 노드들은 수집한 데이터를 트랜잭션으로 만들어 다른 부서 노드들과 검증을 진행한다. 트랜잭션이 일정량 모이게

되면 부서 노드들은 블록을 생성하기 위해 1명의 리더 노드를 선출한다.

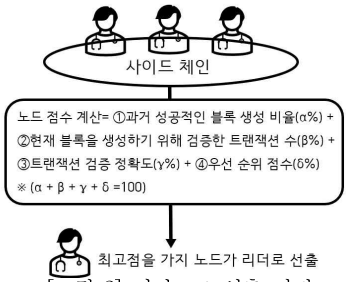
리더 노드는 점수기반으로 선출되며 점수가 가장 높은 부서 노드가 리더 노드가 된다. 리더 노드로 선출된 노드는 블록을 생성할 수 있게 되고 블록 생성에 성공할 시 보상으로 점수 계산 항목으로 들어가는 우선순위 점수를 부여받게 된다. 점수 계산은 [그림2]와 같이 과거 성공적인 블록 생성 비율을 α%, 현재 블록을 생성하기 위해 검증한 트랜잭션 수를 β%, 노드의 트랜잭션 검증 정확도를 γ%, 우선순위 점수를 δ%로 하여 총 4가지 항목을 합산해 계산하며 1:n 상호평가를 통해 산출된다(1<n<부서 노드의 수). 각 부서 노드는 n개의 다른 부서 노드들로부터 점수를 계산 받게 되고, 이들 점수를 평균한 값이 해당 부서 노드의 최종 점수가 된다. 부서 노드들은 각자의 최종 점수를 비교하여 리더 노드를 선출한다. 리더 노드는 블록을 생성할 때마다 점수를 새롭게 계산하여 선출한다.

b. 각 병원의 메인 노드로 구성된 메인 체인 네트워크

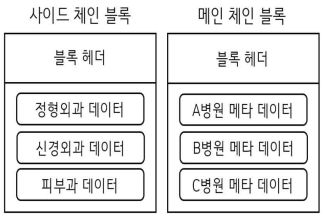
병원마다 1개의 메인 노드가 존재한다. [그림 1]과 같이 메인 노드는 사이드 체인과 메인 체인에 모두 포함되는 노드이다. 메인 노드는 사이드 체인에서 리더 노드를 선출하는 과정에서 제외된다. 하지만 사이드 체인을 구성하는 노드 중 하나이기 때문에 사이드 체인의 분산 원장을 모두 저장하고 있다. 즉 메인 노드는 해당 병원의 모든 데이터를 저장하고 있는 서버 역할을 한다. 메인 노드는 사이드 체인에서 생성된 블록을 자신의 사이드 체인에 연결한 후 해당 블록을 메타 데이터로 압축하여 이를 메인 체인에서 사용한다. [그림 3]과 같이 메인 노드는 메타 데이터를 트랜잭션으로 만들어 다른 병원의 메인 노드들과 검증을 진행한 후 이를 메인 체인 블록에 포함 시킨다.



[그림 1] 사이드 체인과 메인 체인 네트워크



[그림 2] 리더노드 선출 과정



[그림3] 블록 구조

**2. 의료 데이터 요청 및 전달 과정**

다른 병원에서 특정 환자의 데이터를 요청하고 전달받는 과정은 다음과 같다. CA(certificated authority)로부터 메인 노드들은 인증서와 키를 발급받았다고 가정한다.

(가)환자는 A병원의 정형외과에서 진료를 보았다. A병원의 정형외과 부서 노드는 환자의 데이터를 트랜잭션으로 만들어 다른 부서 노드들과 검증한다. 부서 노드들은 일정량의 트랜잭션이 모이면 점수 계산을 진행해 리더 노드를 선출한다. 리더 노드는 (가)환자의 데이터가 담긴 블록을 생성한다. 메인 노드는 이 블록을 자신의 사이드 체인에 연결하고 해당 블록을 메타 데이터로 압축하여 트랜잭션으로 포함 시킨다. 만약 (가)환자가 B병원의 정형외과로 옮겨 수술받게 된다면, 데이터 공유를 위해 B병원은 (가)환자의 의료 데이터를 A병원으로부터 공유받아야 한다. 이를 위한 과정은 다음과 같다.

① B병원의 메인노드는 메인체인에 (가)환자의 데이터가 위치한 노드를 알려달라는 query를 보낸다. 메인체인은 A병원의 메인노드에 있다고 reply를 보낸다.

② B병원의 메인노드는 A병원의 메인노드에게 (가)환자의 데이터를 요청한다.

③ A병원의 메인노드는 정보를 요청한 노드를 인증한다.

④ 인증이 완료되면 A병원의 메인노드는 (가)환자의 데이터를 자신의 사이드체인에서 가져와 데이터를 B병원의 메인노드의 공개키로 암호화하여 이를 B병원의 메인노드로 전송한다

⑤ B병원의 메인노드는 전달받은 데이터를 자신의 개인키로 복호화하여 (가)환자의 데이터를 얻게 된다.

## Ⅳ. 결론

본 연구는 사이드 체인에서 부서별로 환자 데이터를 트랜잭션으로 생성하여 관리하며 리더 노드를 선출하여 블록을 생성한다. 이를 통해 사이드 체인에 저장된 환자의 데이터는 무결성이 보장되며 악의적인 노드들이 접근하여 데이터를 도용하거나 변경할 수 없다. 또한 매번 블록을 생성할 때 점수 기반 방법을 이용하여 리더 노드를 선출하기 때문에 사이드 체인에 기여를 많이 하는 노드가 리더로 선출되게 된다. 그러므로 블록을 생성하는 리더 노드에 대한 신뢰도가 높아지고 다른 노드들도 체인에 기여하려는 구조가 마련된다. 메인체인에서는 쿼리와 요청을 통해 신속하게 무결성이 보장된 환자의 의료 데이터를 다른 병원에서 공유받을 수 있다. 향후 연구로는 사이드 체인 블록을 메타 데이터로 압축하는 부분을 고려하여 효율적이고 신뢰성을 보장할 수 있는 의료 시스템을 제안하고자 한다.


## ACKNOWLEDGMENT

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2023R1A2C1005712)

(교신저자: 도인실)


## 참 고 문 헌


[1] 우성희. (2015). “IoT 환경의 의료 정보보호와 표준 기술, ” 한국정보통신학회논문지, 19(11), 2683-2688

[2] 최성호, 곽진. (2015). “국외 의료기기 보안위협 사례 및 보안 동향 조사, ” 정보보호학회지, 25(3), 11-18

[3] Yaodong Huang, Jiarui Zhang, Jun Duan, Bin Xiao, Fan Ye, Yuanyuan Yang. (2019). “Resource Allocation and Consensus on Edge Blockchain in Pervasive Edge Computing Environments, ” International Conference on Distributed Computing Systems (ICDCS)

[4] Shivani Wadhwa, Gagandeep. (2022). “Lightweight Modified Consensus Approach in IoT Blockchain, ” International Conference on Emerging Smart Computing and Informatics (ESCI)