Journal of Korea Multimedia Society Vol. 25, No. 7, July 2022(pp. 922-931)
https://doi.org/10.9717/kmms.2022.25.7.922

# 하이퍼레저 패브릭과 비대칭키 암호화 기술을 결합한 건강정보 관리서버

한혜경†, 황희정††

# Hyperledger Fabric and Asymmetric Key Encryption for Health Information Management Server

Han Hyegyeong†, Heejoung Hwang††

## ABSTRACT

Recently, the need for health information management platforms has been increasing for efficient medical and IT technology research. However, health information is requiring security management by law. When permissioned blockchain technology is used to manage health information, the integrity is provided because only the authenticated users participate in bock generation. However, if the blockchain server is attacked, it is difficult to provide security because user authentication, block generation, and block verification are all performed on the blockchain server. In this paper, therefore, we propose a Health Information Management Server, which uses a permissioned blockchain algorithm and asymmetric cryptography. Health information is managed as a blockchain transaction to maintain the integrity, and the actual data are encrypted with an asymmetric key. Since using a private key kept in the institute local environment, the data confidentiality is maintained, even if the server is attacked. 1,000 transactions were requested, as a result, it was found that the server's average response time was 6,140ms, and the average turnaround time of bock generation was 368ms, which were excellent compared to those of conventional technology. This paper is that a model was proposed to overcome the limitations of permissioned blockchains.

**Key words:** Health Information, Management Server, Hyperledger Fabric, Asymmetric key, Security

## 1. 서 론

최근 IT기술의 발전으로 다양한 분야에서 인공지능 데이터 분석 기술이 연구되고 학습을 위한 데이터 산업의 규모가 증가하고 있다. 예를 들어 마이데이터 사업처럼 정보주체가 자신의 데이터를 관리, 판매하는 데이터 산업의 필요성도 증가하고 있다[1-3]. 의료 분야에서도 IT기술을 활용하여 개인의 건강정보를 관리할 뿐만 아니라 진단과 예측에 활용하여 의료 서비스의 질을 높이기 위한 연구가 증가하고 있다[4-6].

하지만 국내에서 건강정보를 관리 시스템을 구축하려면 의료법 시행령 제10조 5와 같이 보안 요구사항이 존재한다[7]. 건강정보는 중요한 개인정보로서 불법 접근과 유출을 차단하기 위한 시스템이 필요하다[8]. 따라서 건강정보 관리 시스템의 요구사항을

※ Corresponding Author: Heejoung Hwang, Address: (13120) 1342 Seongnamdaero, Sujeong-gu, Seongnam-si, Gyeonggi-do, Korea, TEL: +82-31-750-4758, FAX: +82-31-750-4758, E-mail: hwanghj@gachon.ac.kr
Receipt date: May 18, 2022, Approval date: Jun. 16, 2022
† Dept. of IT Convergence Engineering, Graduate School, Gachon University (E-mail: gv0mail@gachon.ac.kr)
†† Dept. of Computer Engineering, College of IT Convergence, Gachon University
※ This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2022-2017-0-01630) supervised by the IITP(Institute for Information & communications Technology Promotion)

블록체인 분산원장으로 해결하고자 많은 연구가 진행되고 있다[9-11].

건강정보 관리서버는 사용자를 구분하고 데이터를 저장, 조회, 검색할 뿐만 아니라 기관에서 데이터를 조회하고 판매하는 과정을 지원할 수 있어야 한다. 데이터를 저장하고 관리하기 위해 허가형 블록체인을 이용하면 허가된 사용자만 거래에 참여하기 때문에 상대적으로 적은 연산 능력으로 합의와 검증을 진행하는 블록체인 서버를 구성할 수 있다. 하지만 허가형 블록체인은 거래 참여자 허가와 블록 생성, 검증을 서버에서 관리하기 때문에 분산 시스템의 가용성이 감소하고 블록체인 관리 서버가 공격받으면 보안 효과가 떨어지는 문제가 있다.

블록체인 기반 건강정보 관리서버에 관한 기존 연구에서는 데이터를 관리하는 시나리오를 제안했지만, 블록체인 건강정보 관리 시스템을 구축하기 위한 구체적인 알고리즘은 부족하다[9]. 또 허가형 블록체인을 이용하여 구체적인 건강정보 관리 블록체인 모델을 제안했지만, 블록체인 서버에서 거래에 참여하는 그룹을 관리하기 때문에 블록체인 서버가 공격받으면 취약해지는 한계가 있다[10-11].

따라서 본 논문에서는 허가형 블록체인인 하이퍼레저 패브릭(hyperledger fabric)과 비대칭키를 활용하여 보안 기능을 제공하는 건강정보 관리서버를 제안한다. 하이퍼레저 패브릭은 허가형 블록체인으로 서버의 연산 능력의 낭비를 줄이고 블록체인 알고리즘을 이용하여 공개 또는 기밀 데이터 전송이 가능하여 건강정보를 거래에 참여한 사용자에게만 전송할 수 있다. 비대칭키를 이용하면 블록체인 서버에서 공개키로 암호화하고 개인키를 거래 참여자의 환경에서 관리하면 블록체인 서버에 문제가 발생해도 데이터가 유출되지 않는다.

본 논문에서 제안하는 모델은 하이퍼레저 패브릭을 이용하여 건강정보를 저장하고 거래하는 주체끼리 채널을 생성하여 비밀리에 정보를 교환할 수 있도록 지원한다. 게다가 건강정보는 거래하는 과정에서 공개키를 이용하여 암호화하기 때문에 비밀키 없이는 실제 건강정보가 유출되지 않아 기밀성이 유지된다. 따라서 제안한 모델의 성능을 평가하기 위해 정보 저장 트랜잭션을 발생시키고 응답 시간과 경과 시간을 측정한다. 또 데이터 조회가 발생하면 요청의 무결성을 검증하고 공개키를 조회하는데 걸리는 시간을 측정하여 모델이 효율적으로 건강정보를 관리할 수 있는지 평가한다.

블록체인 기반 건강정보 관리서버를 제안하기 위해서 2장 관련연구에서 블록체인 기술의 장단점과 하이퍼레저 패브릭을 살펴본다. 그리고 3장에서 건강관리서버의 구체적인 동작 시나리오를 제안하고 4장에서 실제로 구현하여 성능과 응답속도를 살펴본다. 5장에서는 본 논문의 의의와 한계를 통해 결론을 맺는다.

## 2. 관련연구

### 2.1 블록체인 분산원장

블록체인 분산원장은 거래 정보를 중앙 서버가 아닌 개인, 각 노드가 관리하는 분산 시스템의 일종으로 블록이라는 데이터 구조에 거래 내역을 저장하고 해시 알고리즘을 이용하여 무결성을 보장한다[12-14]. 해시 알고리즘은 임의의 크기를 가진 데이터를 원문을 추정하기 어려울 정도로 가공하기 때문에 원문을 보호하고 해시값을 비교하여 무결성 침해를 판단할 수 있다. 블록체인 분산원장의 예시는 Fig. 1과 같다.

Fig. 1에서 블록은 블록의 해시 영역(hash of the block)과 블록의 정보가 저장되는 이전 블록해시(previous blockhash)와 시간, 머클루트(time, merkle root), 그리고 거래내역이 저장되는 트랜잭션(transaction)으로 구분된다. 블록 해시 영역은 이전 블록해시와 시간, 머클 루트, 트랜잭션 데이터를 해시 알고리즘으로 이용하여 생성하는 헤더로 각 블록마다 고유한 값을 가진다. 이전 블록해시는 이전 블록의 블록 해시 영역이며, 머클 루트는 트랜잭션 조회를 위한 트리이다. 트랜잭션에는 실제 거래 데이터가 작성되고 가상화폐 이동과 같은 간단한 거래 대신 다양한 내용을 생성하여 블록체인을 무궁무진하게

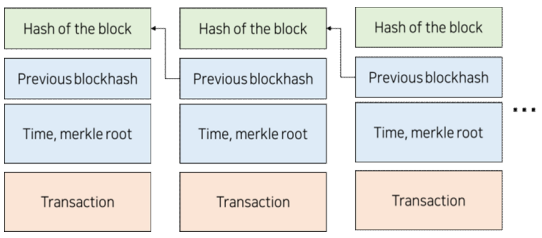


Fig. 1. Blockchain data structure.

활용할 수 있다.

그러나 블록체인을 건강정보 관리서버에 활용하기 위해서는 3가지 문제점을 해결해야 한다[9]. 첫째, 악성 사용자가 악의적으로 트랜잭션을 발생한다면 올바른 데이터와 어떻게 구분할 것인지 판단할 필요가 있다. 둘째, 블록체인을 이용하면 합의하는 과정에서 연산 능력이 낭비될 수 있다. 셋째, 데이터에 위변조가 가해지면 이를 감지하고 처리하기 위한 기술이 필요하다.

한 연구에서는 블록체인 분산원장 기반 건강관리 시스템을 제안하고 있다. 블록체인 서버가 데이터 비즈니스를 위한 연구기관(research institute), 의료법인(medical service provider), 일반 사용자(user device)간의 통신과 데이터 처리, 인증에 관한 시나리오를 제안하였다[9]. 이 연구에서는 건강데이터의 정보 주체가 데이터를 저장, 관리하고 의료법인에 제공할 수 있으며, 판매하여 수익을 올릴 수 있는 시나리오를 제안하고 있다. Fig. 2는 연구에서 제안한 시스템을 간단하게 나타낸 것이다.

이 프레임워크는 데이터를 검색하고(Data search service), 블록에서 데이터 분실이나 위변조를 감지하면 복구(Recovery service)할 수 있다. 블록체인 생성하고 배포하면 발생하는 이벤트를 사용자와 법인에 알려주기 위한 메시지 서비스(Message service)를 제공하고, 네트워크 오버헤드가 발생하지 않도록 효율적인 라우팅(Network service)을 제공한다.

그러나 정작 어떤 블록체인 알고리즘을 이용하는지에 대한 제안이 부족하다. 또 실제 구현을 하지 않아 제안한 프레임워크에 대한 성능 평가가 어렵다. 블록체인 분산원장을 이용해 건강정보 관리서버를 구성하는 경우 3가지 문제에 해결해야 하는데 그에 대한 제안도 부족하다. 따라서 본 연구에서는 적합한 블록체인을 알고리즘을 선정하여 건강정보 관리서버를 제안하고 구현하고자 한다.

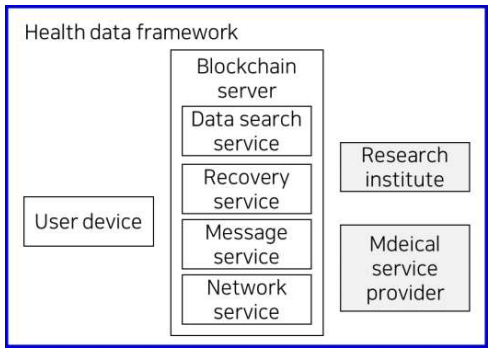


Fig. 2. Health data management framework.

### 2.2 하이퍼레저 패브릭

건강정보 관리서버는 건강정보를 관리의 요구사항을 만족하기 위해서 개인의 건강정보를 저장, 조회, 판매하는 모든 트랜잭션을 비공개 거래 채널에서 처리할 필요가 있다. 또 건강정보가 클라우드 서버에 저장되고 데이터 무결성을 유지하며 허가된 사람에게만 데이터를 공유해야 한다. 따라서 비공개 채널을 지원하며 거래 참여자의 인증이 필요한 허가형 블록체인이 적합하다.

그러므로 가장 많이 이용되는 오픈소스 기반 허가형 블록체인 알고리즘인 하이퍼레저 패브릭에 대해 알아볼 필요가 있다[15]. 하이퍼레저 패브릭은 블록체인 알고리즘으로 법인 간 분산원장 거래에서 거래 내용에 대한 기밀 유지를 제공하기 위해 고안되었다[16]. 참여자가 채널을 생성하여 트랜잭션 내용을 거래 당사자만 확인할 수 있어 건강정보와 같은 민감한 개인 정보를 처리하기에 적합하다[17-18].

하이퍼레저 패브릭 알고리즘의 구성요소는 Fig. 3과 같다. 허가된 사용자 그룹(group)이 클라이언트 요청을 처리하는 피어 노드(peer)를 생성하여 채널(channel)을 구성한다. 채널에서는 피어 노드 간의 트랜잭션이 발생하고 오더러(orderer)로 데이터를 전송한다. 오더러에서는 트랜잭션을 검증하고 블록을 생성하여 블록체인 서버에 연결한다. 그룹은 피어와 채널을 여러 개 생성할 수 있어 확장성이 높다.

Fig. 4는 하이퍼레저 패브릭 알고리즘에서 트랜잭션 처리 과정을 나타낸 그림이다. 예를 들어 클라이

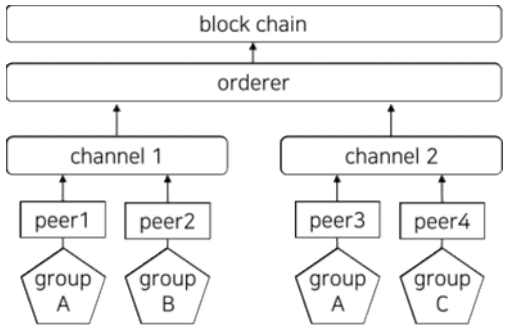


Fig. 3. Hyperledger fabric flowchart.

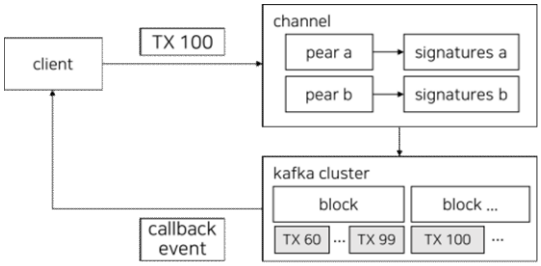


Fig. 4. Hyperledger fabric blockchain algorithm.

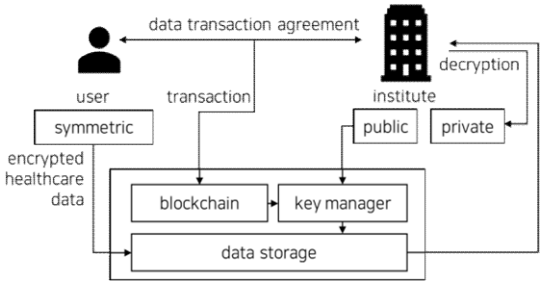


Fig. 5. Blockchain data transaction process.

언트(client)가 100번째 트랜잭션(TX100)을 요청하면 채널에서는 채널에 참여하는 피어들이 트랜잭션이 유효한지 검사하고 결과를 카프카 클러스터로 보낸다. 카프카 클러스터는 다른 오더 노드에도 검증을 마친 다음에 블록에 트랜잭션을 삽입하고 블록의 무결성을 관리한다. 피어 노드에서 트랜잭션의 유효성을 검사하고 무결성 유지에는 다른 그룹의 노드들도 참여하기 때문에 전체 블록의 무결성 검증 성능은 증가하지만, 트랜잭션의 내용은 거래의 참여한 피어 노드에서만 확인할 수 있다.

결과적으로 각각의 클라이언트는 블록 관리를 고려할 필요 없이 채널에 트랜잭션을 발생하기만 하면 거래 데이터의 무결성을 유지할 수 있다. 하이퍼레저 패브릭은 그룹 사용자마다 각각의 채널을 생성하여 비밀 원장을 구성할 수 있기 때문에 데이터 기밀성이 필요한 금융 거래나 건강정보 처리에 적합하다[16]. 따라서 본문에서 하이퍼레저 패브릭을 이용한 건강정보 관리서버를 제안하고자 한다.

## 3. 블록체인 기반 건강정보 관리서버

### 3.1 건강정보 관리서버 개요

본 논문에서는 블록체인 알고리즘 하이퍼레저 패브릭을 이용한 건강정보 관리서버를 제안한다. 건강정보 관리서버는 사용자의 건강정보를 암호화하여 저장하고 조회가 허가된 기관에게 데이터를 제공하는 기능을 지원해야 한다. 사용자와 기관 사이의 조회 동의 거래는 트랜잭션으로 블록체인 서버에 저장되어 무결성을 유지하고 사용자 정보를 복호화하기 위한 대칭키를 기관의 공개키로 암호화하여 전송하여 기밀성을 유지한다.

Fig. 5는 사용자가 건강정보를 저장하고 기관에 정보를 제공하는 과정이 간략하게 나타낸 그림이다. 사용자는 데이터마다 각각의 대칭키(symmetric)로 암호화하여 저장소(data storage)에 저장한다. 그리고 허가된 기관에서 사용자에게 건강정보를 요청하면 사용자의 동의 여부를 블록체인 서버에 저장하여 거래 무결성을 유지한다. 이후 사용자의 대칭키는 기관의 공개키(public)로 암호화되어 기관에 전달되고 기관에서는 개인키(private)로 데이터를 복호화하여 사용자의 건강정보를 확인한다.

Fig. 5와 같이 서버를 구성하면 블록체인 분산원장을 이용하여 거래 무결성을 유지하고 비대칭키와 대칭키 암호화 알고리즘을 적절하게 활용하여 기밀성을 유지하게 된다. 허가형 블록체인은 블록체인 서버가 취약하면 보안 성능이 떨어지는 한계가 있는데, 비대칭키로 기밀성을 유지하기 때문에 기관의 개인키와 블록체인 서버가 동시에 공격받아야 사용자 데이터가 유출되기 때문에 더 안전하게 건강정보를 관리할 수 있다. 또 비대칭키와 상대적으로 속도가 빠른 대칭키 암호화 알고리즘을 적절하게 사용하여 암복호화에 걸리는 시간을 효과적으로 관리한다.

Fig. 6는 건강정보 관리서버의 기능을 지원하기 위해 서버의 구성도를 나타낸 그림이다. 그림에서 블록체인 헬스케어 서버(health information manage-

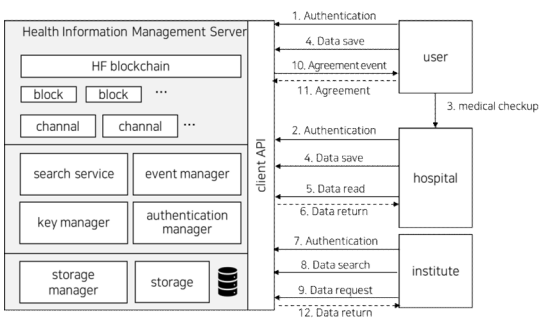


Fig. 6. Health information management server.

ment server, HIMS)와 클라이언트 영역으로 구분할 수 있다. 먼저 클라이언트는 건강정보의 주체가 되는 사용자(user)와 건강정보를 측정하고 저장하는 병원(hospital) 그리고 건강정보를 검색하고 구매하는 관련 기관(institute)으로 구분된다.

먼저 서버에 개인 사용자가 본인의 키를 발급받는 인증(authentication)과정을 진행한다. 데이터를 저장하고 조회, 판매하는 과정에서 사용자의 키로 데이터 제공에 동의했다는 것을 확인한다. 병원에서는 허가된 병원이라는 인증을 거친 후에 블록체인 서버에 체인을 생성하는 참여자로 연결된다. 기관은 병원과 같이 인증된 단체지만 건강정보를 검색하고 정보주체에게 요청하여 비용을 지불한 뒤에 데이터를 조회할 수 있다.

블록체인 서버에서는 데이터 저장, 조회, 판매 시나리오마다 블록을 생성하거나 검사하여 데이터를 안전하게 관리한다. 먼저 정보주체에게 허가된 경우에만 데이터를 저장, 조회하는 스토리지 매니저(stroage manager) 기능을 제공한다. 스토리지 데이터를 활용하기 위해 서버에서는 인증 매니저(authentication manager)와 검색 서비스(search service), 이벤트 매니저(event manager), 키 매니저(key manager) 기능을 제공한다.

인증 매니저는 사용자 암호를 이용하여 사용자를 구분하고 발생한 트랜잭션의 유효성을 확인하고 스토리지 매니저에게 데이터를 요청하는 기능을 제공하는 서비스이다. 검색 서비스는 건강정보 데이터 구조를 검색하여 건강정보가 필요한 관련 기관이 데이터를 조회하고 요청할 수 있도록 서비스를 제공한다. 키 매니저는 클라이언트의 요청에 따라서 관련 기관의 공개키를 관리하고 공개키로 데이터를 암호화하는 기능을 제공하게 된다. 이벤트 매니저는 동의를 비롯한 각종 이벤트가 발생했을 때 개개인에게 알림을 보내고 결과를 받아오는 기능을 제공한다. 각 과정에서 생성된 건강정보와 건강정보 제공 동의는 블록체인으로 저장되어 무결성을 유지한다.

건강정보 관리서버에서 블록체인을 생성하는 채널은 아래 Fig. 7과 같다. 건강정보를 저장할 때는 채널 A와 채널 B에 트랜잭션이 발생한다. 채널 A에는 건강정보 데이터를 조회할 수 있는 데이터 아이디를 저장하고, 채널 B에는 건강정보 데이터 구조를 저장하고 관련 기관이 데이터 검색 서비스를 이용할 수 있도록 구성한다. 관련 기관에서 데이터 검색 서비스를 이용하여 원하는 건강정보를 선정한 다음 정보주체에게 제공을 요청할 수 있다. 정보주체에게 데이터를 요청하고 그 결과로 데이터를 받아온 거래내역을 채널 C에 블록체인으로 생성하여 관련 기관에서 스토리지 매니저로 데이터를 조회하게 된다.

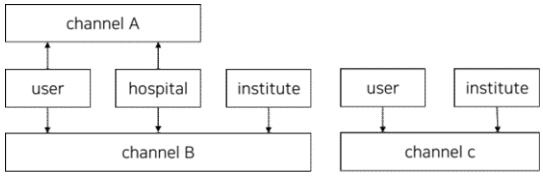

Fig. 7. Hyperledger fabric channel.

건강정보 관리서버는 건강정보를 저장하고 조회할 수 있으며, 허가된 관련 기관에게 데이터를 판매할 수 있다. 서비스를 제공하는 각 과정에 블록체인 알고리즘과 개인 인증 방식으로 기밀성과 무결성을 유지한다. 다음 절에서 데이터 저장하는 시나리오를 정의하고 나서 데이터를 조회, 판매하는 시나리오를 각각 제시한다.

### 3.2 데이터 저장 시나리오

데이터 저장 시나리오는 정보주체인 개인 사용자가 병원에서 건강정보를 측정하면 HIMS에서 데이터를 저장하는 과정이다. HIMS는 악성 사용자의 악의적인 트랜잭션을 올바른 트랜잭션과 구분할 필요가 있다. 본 논문에서는 데이터 저장을 Fig. 8과 같이 사용자가 병원에서 의료적 진단을 진행하고 생성된 건강정보를 인증 매니저로 검사한 후에 저장하고 관리하는 기능을 제공한다.

먼저 건강주체를 구분하기 위해 인증 매니저에서 사용자 인증을 진행하여 개인이 설정한 암호에 따라서 대칭키를 발급받는다. 측정한 건강정보를 사용자의 대칭키로 암호화하여 블록체인 서버에 전송하면 사용자와 허가된 병원 기관에서 보낸 것인지 인증 매니저로 검사한다. 검사 결과 허가된 병원에서 측정된 데이터라면 스토리지에 암호화된 건강정보를 저장하고 트랜잭션으로 채널 A와 채널 B에 기록한다. 이때 채널 A에는 스토리지 매니저로 데이터를 조회할 수 있는 데이터 아이디를 저장하고, 채널 B에는 데이터 구조를 저장하여 다른 기관에서 데이터를 검색할 수 있도록 구성한다.

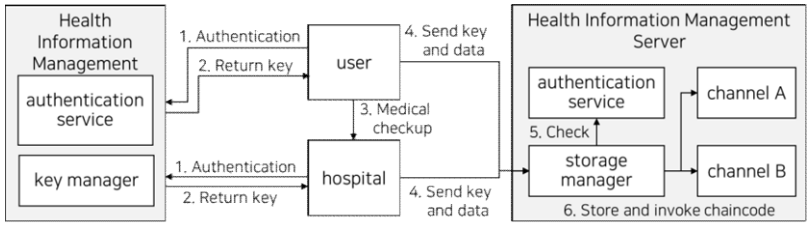


Fig. 8. Health information recording scenario.

HIMS에서는 데이터를 저장하고 저장 정보를 블록으로 관리하기 때문에 무결성을 유지할 수 있다. 그러나 정보를 조회하는 과정도 올바른 트랜잭션인지 검사하고 조회 기록을 저장할 필요가 있다.

### 3.3 데이터 조회 시나리오

HIMS는 허가된 클라이언트의 요청이 있을 때 적절한 데이터를 제공할 수 있어야 한다. Fig. 9는 병원에서 사용자의 건강정보를 확인하는 과정을 나타낸 그림이다. HIMS는 건강정보를 제공하는 과정에서 정보를 제공하는 주체의 동의를 얻어야 하며, 블록체인을 이용하여 트랜잭션의 무결성을 검증한다. 건강정보 제공 동의를 확인한 뒤에 정보를 제공하며 반환된 건강정보는 기관의 비밀키로 복호화할 수 있도록 구성한다.

먼저 병원에서 블록체인 서버에 정보 조회를 요청하면 스토리지 매니저에서는 정보주체가 동의한 적이 있는지 검사하고, 이벤트 매니저를 통해 사용자에게 동의를 요청한다. 사용자가 정보제공에 동의하면 이벤트 매니저에서는 키 매니저에게 요청하여 수신한 사용자 암호를 검사하고 결과를 반환한다. 인증 매니저는 유효한 거래로 판단하면 사용자 동의를 블록체인 채널에 기록하고 스토리지에 저장된 데이터를 요청한 병원에게 반환한다.

이와 같은 과정을 통해 악성 사용자가 악의적인 트랜잭션을 보내더라도 사용자 암호를 모르면 블록에 추가되지 않아 블록체인을 안전하게 구축할 수 있다. 블록체인은 해시 알고리즘으로 무결성을 유지하여 잘못된 건강정보가 전달되어 문제가 생기지 않도록 검사하는 기능을 제공한다. 또 데이터를 분산 저장하고 인증 절차로 제공하기 때문에 건강정보를 생성한 병원이 아니더라도 쉽게 데이터를 확인할 수 있다.

HIMS를 이용하면 건강정보를 안전하게 저장, 조회할 수 있다. 그러나 이 데이터에 대한 조회를 요청하기 위해서는 데이터를 검색하고 정보주체인 사용자에게 데이터 제공 동의 요청을 할 수 있어야 한다. 다음 절에서는 데이터 판매를 위한 시나리오를 제안한다.

### 3.3 데이터 판매 시나리오

HIMS는 저장된 건강정보를 허가된 기관에게 판매할 수 있는 기능을 지원해야 한다. Fig. 10는 허가된 기관에서 데이터를 검색하고 정보주체에게 정보제공 동의를 얻는 과정을 나타낸 그림이다. 기관은 건강정보 데이터 구조를 확인하고 정보제공을 요청

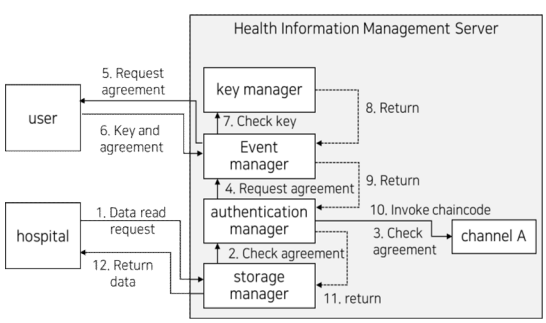


Fig. 9. Health information provide scenario.

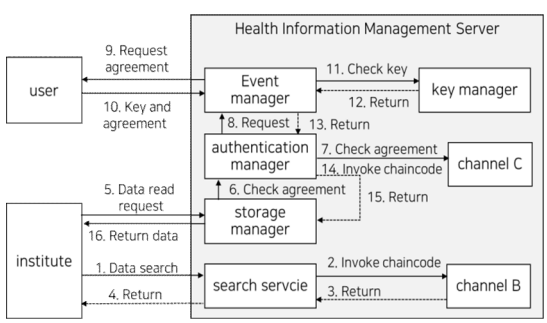


Fig. 10. Health information business scenario.

할 수 있으며 사용자는 정보를 제공하여 대금을 지불받을 수 있다.

기관에서 검색 서비스를 이용하여 블록체인 채널 B에 저장된 데이터 구조를 검색한다. 기관은 HIMS에 어떤 종류의 건강정보 데이터가 얼마나 있는지 파악할 수 있다. 기관은 HIMS에 데이터를 요청하면 스토리지 매니저에서는 기관이 데이터에 접근할 권한이 있는지 확인한다(check agreement). 트랜잭션에서 접근 권한이 있는 것으로 확인되면 스토리지 매니저를 통해 데이터를 반환한다.

만약 해당 기관에서 데이터에 접근할 권한이 없다면 정보주체에게 이벤트 매니저를 이용하여 정보이용 동의 요청을 전달한다. 정보주체인 사용자는 정보제공 동의 요청을 받고 개인 암호를 이용하여 정보제공에 동의할 수 있다. 이벤트 메니저는 건강정보 제공 동의를 반환받으면 인증 매니저를 이용하여 올바른 사용자가 정보제공에 동의한 것인지 확인한다.

올바른 사용자가 정보제공에 동의한 것으로 확인되면 정보거래 내용을 채널 C에 트랜잭션으로 발생하여 저장한다(invoke chaincode). 또 이 과정에서 건강정보 복호화에 필요한 키를 기관의 공개키로 암호화하여 기관에게 전달한다. 이때 기관은 사용자에게 대금을 지불할 수 있도록 서비스를 제공한다. 기관은 제공받은 데이터로 연구를 진행하여 다시 의료서비스의 질을 높이는데 기여할 수 있을 것이다.

HIMS는 관련연구에서 제안한 3가지 문제점을 만족한다. 허가된 사용자와 기관만 참여하고 인증 매니저를 통해 첫 번째 문제점인 악성 사용자의 악의적인 트랜잭션을 거부할 수 있다. 또 하이퍼레저 패브릭은 허가된 사용자만 트랜잭션에 참여하기 때문에 적은 연산 능력으로 무결성을 유지하여 컴퓨팅 파워가 낭비되는 두 번째 문제를 해결한다. 또 데이터를 검증하고 사용자 암호를 이용하여 암복호화하므로 데이터에 위변조가 발생하더라도 사용자 암호로 감지하기 때문에 데이터의 위변조를 감지해야 하는 세 번째 문제점을 해결하게 된다. 그러므로 HIMS를 실제로 구축하고 그 성능을 평가할 필요가 있다.

## 4. 실험 결과 및 분석

블록체인은 그 구조에서 해시 알고리즘을 통해 생성한 값을 아이디로 사용하여 무결성을 유지하게 된다. 그리고 데이터 스토리지에 저장하는 과정에서 사용자 암호에 기반한 대칭키로 암호화하기 때문에 기밀성이 유지된다. 하지만 블록체인을 생성하는 과정에서 너무 많은 시간이 소요된다면 서버의 신뢰성과 사용성이 떨어지게 된다. 따라서 블록체인 기반 건강정보 관리서버의 성능을 평가하기 위해서는 블록체인이 만들어지는 과정에서 연산 능력이 낭비되지 않는지 평가할 필요가 있다.

HIMS는 Fig. 11과 같이 트랜잭션을 요청하면 올바른 요청인지 인증 정보를 검사하고, 블록체인 서버에서 트랜잭션을 생성한 다음 배포하고 결과를 반환해야 한다. 본 실험에서는 서버 API(application programming interface)의 성능을 평가하기 위해 하나의 사용자가 10번, 250번, 500번, 1000번을 동시에 요청하는 상황에서 처리에 걸리는 시간을 측정하였다.

HIMS는 하이퍼레저 패브릭 기반 블록체인 서버 API 플랫폼인 Kaleido[19]를 이용하여 Fig. 11에서 제안한 시나리오가 동작하도록 구현하였다. 블록체인 서버는 Kaleido의 자체적인 기준으로 vCPU 0.5, 1GB 메모리를 할당하고 성능 평가 실험을 진행하였다. HIMS에 Fig. 11의 과정을 요청하는 클라이언트는 Talend API Tester[20]를 이용하여 실험하였다.

실험 결과 서버가 응답에 걸린 시간을 Fig. 12에서 그래프로 표현하였다. 응답시간은 서버에서 사용자를 인증한 다음 체인코드를 통해 트랜잭션을 생성하고 결과를 반환하는데 걸리는 시간으로 10회의 요청에서는 평균 688 ms로 응답되는 것을 확인하였다. 그러나 250번의 요청이 발생했을 때는 약 두 배인 1,243 ms로 측정되었고, 1,000번의 요청이 동시에 발생하였을 때는 6,140 ms로 10번에 비교해 약 10배 가까이 증가하였다.

Fig. 12에서 응답시간이 10번은 688 ms에서 1,000

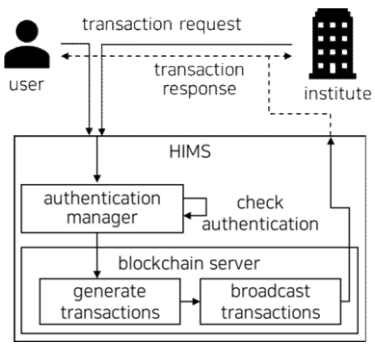


Fig. 11. HIMS performance experiment scenario.

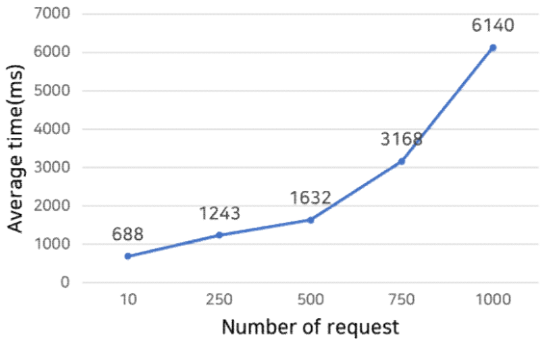


Fig. 12. Server response time.

번은 6,140 ms로 약 10배 증가한 원인을 분석할 필요가 있다. 동작 과정은 API로 서버에서 요청하면 블록체인 서버에서 처리하고 결과를 반환하기 때문에 API 서버의 메모리가 부족해서 응답이 지연된 문제일 수도 있고, 블록체인 서버에서 처리 시간이 증가한 문제일 수도 있다. 그러므로 정확한 성능을 평가하기 위해 Fig. 13에서 HIMS 내부 블록체인 서버에서 체인코드를 동작하는데 걸리는 시간을 분석하였다.

Fig. 13은 HIMS 내부에서 블록체인을 생성하는데 소요한 시간을 요청 트랜잭션 수에 따라서 그래프로 나타낸 것이다. 동시에 발생한 10개의 트랜잭션을 블록으로 생성하는데 처리 시간은 평균 341 ms로 측정되었으며, 250개는 342 ms, 500개는 348 ms, 750개는 355 ms, 1,000개는 368 ms로 측정되었다. 결과적으로 Fig. 13 보면 블록 생성에 필요한 평균 처리 시간은 Fig. 12의 응답 시간과 비교해 근소하게 증가한 것을 확인할 수 있다. 따라서 Fig. 12에서 보이는 1,000개의 요청이 10개의 요청보다 약 10배에 해당하는 시간이 걸리는 이유는 블록체인의 구조적 문제보다 REST API 서버의 연산 능력 문제로 판단할 수

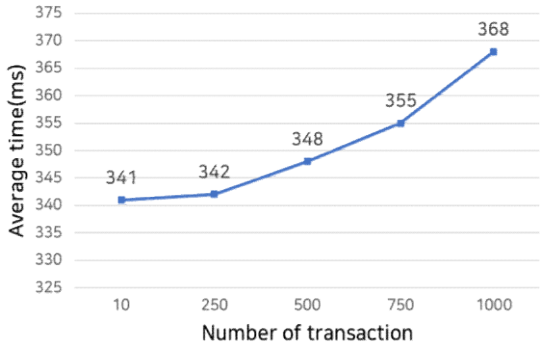


Fig. 13. Transaction turnaround time.

있다.

게다가 기존 연구에서는 블록체인 서버의 부하를 평가하기 위한 실험에서 같은 하이퍼레저 패브릭 알고리즘을 사용하였을 때, 500개의 블록을 생성하는데 평균 318 ms, 1,000개의 블록을 생성하는데 평균 450 ms로 132 ms가 증가하였다[11]. 본 연구에서 실험한 블록체인 처리 시간은 500개에서 348 ms지만 1,000개에서 368 ms로 약 20 ms 증가하여 기존 기술보다 부하에 효과적인 것을 확인하였다. 실제 환경에서 1,000개의 트랜잭션이 동시에 발생할 가능성은 낮고 서버 성능이 낮은 것을 고려하면 API 응답시간과 트랜잭션 처리 시간을 통해 본 논문에서 제안한 건강정보 관리서버가 유효성이 있음을 확인하였다.

## 5. 결 론

건강정보를 분석하여 진단과 예측에 활용하면 의료 서비스의 질을 높일 수 있다. 그러나 건강정보를 통합하고 허가된 기관에게 데이터를 제공하기 위한 플랫폼은 건강정보를 안전하게 관리할 필요가 있다. 건강정보 관리서버에 블록체인을 활용하면 데이터 무결성을 높일 수 있지만, 블록체인을 합의하는 과정에서 연산 능력이 낭비되고 사용자 인증의 문제가 발생한다. 또 블록체인 관리 서버에서 인증과 연산 능력을 제공한다면 블록체인과 같은 분산형 시스템의 특징인 가용성과 보안 능력이 감소하는 문제가 있다.

따라서 본 연구에서는 허가형 블록체인 기반 건강정보 관리서버는 건강정보의 보안을 위해 블록체인 기술과 비대칭키 기술을 사용한다. 허가형 블록체인을 사용하기 때문에 서버의 무결성을 유지하면서 연산 능력의 낭비는 감소하고, 비대칭키를 사용하여 허가형 블록체인이 블록체인 서버가 공격받으면 데이터 유출에 취약해지는 점에 대응할 수 있다. 하이퍼레저 패브릭 블록체인을 기반으로 실험한 결과 서버에서 응답 시간은 1,000번 평균 6140 ms이고 블록체인을 1,000개 생성하는 경과 시간은 368 ms로 측정되어 그 유효성이 확인되었다.

본 연구에서는 제안된 아이디어에 따른 서버 구축 결과에 따른 성능 평가를 경과 시간과 서버 API의 응답 시간으로 진행하였다. 향후 연구로는 실제 서비스 이용 환경까지 고려해 UI(user interface) 및 사용자 상호작용 까지를 포함한 전반적인 성능향상 방안

에 관해 연구할 계획이다.

## REFERENCE


[1] J.A. Han and W.S. Na, "A Study on the Smart Healthcare Health Management System," *Journal of Convergence for Information Technology*, Vol. 10, No. 6, pp. 8-13, 2020.

[2] S. Park, S. Ryoo, and S.-Y. Dong, "Responsive Healthcare System for Posture Correction Using Webcam-Based Turtle Neck Syndrome Discrimination Algorithm," *Journal of Korea Multimedia Society*, Vol. 24, No. 2, pp. 285-294, 2021.

[3] H.S. Wi and B.M. Lee, "Customized Realtime Control of Sleep Induction Sound based on Brain Wave Data," *Journal of Korea Multimedia Society*, Vol. 23, No. 2, pp. 204-215, 2020.

[4] H. Kim and M. Yi, "A Study on the Policy Trends for the Revitalization of Medical Big Data Industry," *Journal of Digital Convertgence,* Vol. 18, No. 4, pp. 325-340, 2020.

[5] J. Choi, "Utilization Value of Medical Big Data Created in Operation of Medical Information System," *The Journal of the Korea Institute of Electronic Communication Sciences*, Vol. 10, No. 12, pp. 1403-1410, 2015.

[6] S. Jeong, M. Lee, and S. Yoo, "Machine Learning-based Stroke Risk Prediction Using Public Big Data," *Journal of Advanced Navigation Technology*, Vol. 25, No. 1, pp. 96-101, 2021.

[7] Korea Ministry of Government Legislation, *Enforcement Decree of the Medical Service Act,* 2019.

[8] K.H. Hong, B.M. Lee, and Y.J. Park, "Realtime Individual Identification Based on EOG Algorithm for Customized Sleep Care Service," *Journal of Convergence for Information Technology*, Vol. 9, No. 12, pp. 8-16, 2019.

[9] J. Moon and D. Kim, "Design of a Personal-Led Health Data Management Framework Based on Distributed Ledger," *The Journal of Society for e-Business Studies,* Vol. 24, No. 3, pp. 73-86, 2019.

[10] Y.J. Choi and K. Kim, "Secure Healthcare Data Management and Sharing Platform Based on Hyperledger Fabric," *Journal of Internet Computing and Services*, Vol. 21, No. 1, pp. 95-102, 2020.

[11] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based Electronic Healthcare Record System for Healthcare 4.0 Applications," *Journal of Information Security and Applications*, Vol. 50, No. 102407, 2020.

[12] N. Yoo and D. Yang, "A Study on Blockchain-based Methods for Integrity Verification of Dataset in Relational and NoSQL DBMS," *The Journal of Korean Institute of Next Generation Computing*, Vol. 17, No. 5, pp. 75-87, 2021.

[13] H.J. Kim, K.H. Han, and S.S. Shin, "Chaincode-based File Integrity Verification Model," *Journal of the Korea Convergence Society*, Vol. 12, No. 4, pp. 51-60, 2021.

[14] K.W. Bae and K.H. Lee, "Security of Database Based on Hybrid Blockchain," *Journal of The Korea Internet of Things Society*, Vol. 6, No. 1, pp. 9-15, 2020.

[15] A Blockchain Platform for the Enterprise (2020), https://hyperledger-fabric.readthedocs.io/en/release-2.2 (accessed April 14, 2022).

[16] J.S. Park and S.U. Shin, "Analysis of Blockchain Platforms from the Viewpoint of Privacy Protection," *Journal of Internet Computing and Services,* Vol. 20, No. 6, pp. 105-117, 2019.

[17] H. Choi, "A Study on Application of Blockchain Platform to Trade Process based on Hyperledger Fabric," *Korea Association for International Commerce and Information,* Vol. 23, No. 2, pp. 3-20, 2021.

[18] J.G. Park, S.G. Kwon, K.R. Kwon, and S.H. Lee, "A Research on the Use of DID Using a Private Blockchain," *Journal of Korea Multimedia Society*, Vol. 24, No. 6, pp. 760-767,

2021.
[19] Kaleido(2021), https://www.kaleido.io (accessed April 14, 2022).
[20] Talend(2021), https://www.talend.com (accessed April 14, 2022).

한 혜 경

2020년 가천대학교 IT융합대학 컴퓨터공학과 학사
2020년～현재 가천대학교 대학원 IT융합공학과 컴퓨터공학 전공
관심분야: 스마트 헬스케어, 사물인터넷(IoT), 센서네트워크, 지능형네트워크, 스마트 서비스

황 희 정

2000년 인하대학교 컴퓨터공학과 (공학석사)
2008년 인천대학교 컴퓨터공학과 (공학박사)
2000년～현재 가천대학교 IT융합대학 컴퓨터공학과

관심분야: Software Engineering, u-Health, Big Data, MedicalInformatics, Ubiquitous Computing