http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.24, No.3, August 2019, pp.73-86
https://doi.org/10.7838/jsebs.2019.24.3.073

분산 원장 기반의 개인 주도적 건강 데이터 관리 프레임워크 설계

Design of a Personal-Led Health Data Management Framework Based on Distributed Ledger

문준호(Junho Moon)*, 김동수(Dongsoo Kim)**

초 록

4차 산업 혁명이 시작되고 헬스케어 분야 역시 신기술을 접목한 새로운 비즈니스 모델을 찾기 위해 노력하고 있다. 그중 블록체인 기술은 의료 분야에서 큰 관심을 갖는 기술 중 하나이다. 여러 가지 문제들로 인하여 시장성 확보에 어려움을 겪고 있는 개인 건강 기록 시스템 분야 역시 블록체인 기술의 접목을 통해 시스템의 발전과 시장성 확보를 위한 노력을 기울이고 있다. 하지만 블록체인은 개인 건강 기록 시스템의 문제를 해결하기에는 한계가 있다. 이에 본 연구에서는 블록체인의 상위 개념인 분산 원장 기술을 기반으로 정보 주체가 개인 건강 데이터에 대한 온전한 소유권을 확보할 수 있는 개인 주도적 건강 데이터 관리 프레임워크를 설계하였다. 프레임워크의 설계를 위해 컨소시엄 블록체인 중 하나인 R3 Corda의 구조를 참고하였으며, 개인 사용자의 모바일 장치에 노드를 운용할 수 있도록 기존 블록체인과 다른 네트워크 구조를 설계하였다. 이를 통해 정보주체가 직접 자신의 정보를 저장 및 관리하고 허가된 네트워크 구성원들에게 정보를 공유할 수 있도록 하였다. 제안된 시스템을 통해 의료 산업의 정보 활용도를 향상시키고 국민 건강 증진과 의료 기술의 발전을 이룰 수 있을 것이다.

ABSTRACT

After the 4th industrial revolution, the healthcare industry is striving to find new business models through new technologies. Among them, blockchain technology is one of the technologies that have great interest in the healthcare industry. Most providers of personal health record systems have difficulty in securing marketability due to various problems. Therefore, they try to integrate blockchain technology to develop new systems and gain marketability. However, blockchain has limitations in solving the problems of the personal health record system. In this study, we have designed a personalized health data management framework that enables information subjects to acquire full ownership rights of individual's health data, based on distributed ledger technology. For the framework design, we refer to the structure of R3 Corda. It was designed with a different network structure than the

이 논문은 2017년 대한민국 교육부와 한국연구재단의 이공학개인기초연구지원사업의 지원을 받아 수행된 연구임 (NRF-2017R1D1A1B05029080).

* First Author, Department of Industrial and Information System Engineering, Soongsil University (jhmoon@soongsil.ac.kr)

** Corresponding Author, Department of Industrial and Information System Engineering, Soongsil University (dskim@ssu.ac.kr)

Received: 2019-05-31, Review completed: 2019-07-24, Accepted: 2019-08-01

existing blockchain systems so that the node can be operated on the personal user's mobile device. This allows information subjects to directly store and manage their own data and share data with authorized network members. Through the proposed system, the information utilization of the healthcare industry can be improved and the public health promotion and medical technology development can be realized.

키워드 : 개인 건강 기록, 블록체인, R3 코다, 분산 원장
Personal Health Record, Blockchain, R3 Corda, Distributed Ledger

1. 서 론

2016년 세계경제포럼(World Economic Forum, WEF)에서 언급된 4차 산업혁명은 우리 사회에 많은 변화를 가져다주고 있다. 이에 산업계와 학계 모두 변화에 대응하기 위한 준비에 분주하다. 그 중심에 있는 핵심 기술로는 5G 통신 기술, 자율주행차, 로봇, 인공지능, 빅데이터, 사물인터넷, 모바일, 가상현실, 블록체인, 핀테크, 드론, 3D 프린터 등이 대표적이다. 특히 블록체인 기술은 2017년 비트 코인 가격의 급상승으로 인하여 금융 분야를 중심으로 빠르게 발전하였으며, 4차 산업혁명의 주요 기술로 부상하였다 [4, 5, 11, 13].

의료 산업 역시 블록체인이라는 새로운 기술을 도입하기 위해 다양한 형태의 연구를 진행 중에 있으며, 실제 기술을 적용한 사례들이 속속 등장하고 있다. 딜로이트는 헬스케어 분야에서 블록체인을 활용할 다섯 가지 방안으로써 첫 번째로 의약품 공급망 관리, 두 번째로 임상시험 데이터 공유, 세 번째로 의료 기록의 신속한 업데이트, 네 번째로 개인 주도 의료 정보 관리, 다섯 번째로 보험 의료 사기 방지를 제시하였다. 특히 개인 건강 기록 시스템에 블록체인 기술을 접목함으로써 개인 건강 기록에 대한 사용자의 자기 결정권 및 재산권 확보, 보안성 강화 등 기존 시스템의 개선을 위한 시도가 이루어지고 있다 [10]. 하지만 블록체인 기술의 보안성 문제가 계속해서 제기되고 있으며, 블록체인 기술의 제약조건들로 인하여 해결되지 않은 개인 건강 기록 시스템의 문제점들이 남아있다. 또한, 국・내외 개인정보보호법 및 의료관련 법률로 인하여 실제 적용의 가능성이 희박해 보인다.

이에 본 연구에서는 블록체인기술의 근간인 분산 원장 개념을 활용하여 정보주체(처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람)가 직접 자신의 정보를 소유하고 쉽게 관리할 수 있는 개인 주도적 건강 정보 관리 프레임워크를 설계하였다. 또한, 제안 프레임워크의 활용으로 건강 정보의 활용도를 향상시킬 수 있는 시나리오들을 제시하였으며, 각 시나리오를 토대로 제안 시스템의 기대효과를 기술하였다.

2. 관련 연구

2.1 개인 건강 기록

개인 건강 기록(Personal Health Record: PHR)은 1978년부터 사용되기 시작한 용어로, 개인 건강 기록에 대한 정의는 여러 기관에서

서로 다르게 정의하고 있다. 그중 대체적으로 타당한 정의로 평가 받고 있는 The Healthcare Information and Management System Society (HIMSS)의 정의에 따르면 PHR은 “본인이나 가족의 일생 동안의 모든 건강 정보에 대해서 안전하게 보관하면서 관리하는 기능을 제공하는 도구”를 의미한다[1].

체계적인 개인 건강 기록을 위해 다양한 도구들이 개발되었으며, 다양한 기관에서 각 도구의 형태에 따라 서로 다른 분류체계를 만들었다. 그중 2005 Symposium of the American College of Medical Informatics에서 정리한 분류 방법이 전자화 되어가는 개인 건강 기록 시스템을 가장 잘 분류한 것으로 평가 받고 있다. 이 분류 방법에 따르면 개인 건강 기록 시스템은 의료 기관의 Electronic Medical Record (EMR) 혹은 Electronic Health Records(EHR) 시스템에 종속적인 Tethered-PHR 형태와 의료 기관의 정보가 제외된 개인 건강 정보만을 포함하는 Standalone-PHR, 마지막으로 의료기관의 정보와 그 외의 개인 건강 정보를 모두 포함하는 Interconnected-PHR의 형태로 나뉜다. 그 중 다양한 정보를 포함하고 있는 Interconnected- PHR의 형태가 대부분의 주요 특징에서 효율성이 높다고 평가되었다[15]. 이에 구글, 애플, 마이크로소프트 등 다양한 IT 기업들이 Interconnected-PHR의 형태의 개인 건강 기록 시스템의 연구 및 개발을 진행하였으며, 플랫폼 형태의 평생 건강관리 인프라를 구축하였다. 하지만 기존의 중앙 집중식 데이터 관리 방식을 사용한 개인 건강 기록 시스템은 산재되어 있는 건강 정보의 수집 어려움, 이기종 간의 표준 불일치, 데이터 위・변조의 위험성, 데이터 보안의 위험성, 데이터 활용도 부족 등의 이유로 시장성 확보에 어려움을 겪고 있다[10].

2.2 분산원장과 블록체인

분산 원장 기술은 거래 정보를 기록한 원장을 특정 기관의 중앙 서버가 아닌 P2P(Peer-to-Peer) 네트워크에 분산하여 참가자가 공동으로 기록하고 관리하는 기술을 의미하며, 기존 중앙 집중형 시스템에 비해 효율성, 보안성, 시스템 안정성, 투명성 측면에서 장점을 갖는다. 하지만 신뢰를 담보할 외부 기관이 존재하지 않기 때문에 원장에 기록된 정보의 신뢰성을 확보할 수 있는 메커니즘의 설계가 필요했다[3].

2008년 11월 사토시 나카모토라는 정체불명의 인물이 발표한 비트코인이라는 논문에서 언급한 작업증명을 통한 거래의 신뢰 형성은 분산 원장 기술의 신뢰성 확보 문제를 해결하였다. 새로운 형태의 분산 원장 기술의 등장은 기존의 정보 시스템 생태계에 큰 변화를 불러 일으켰다. 개인 건강 기록 시스템 역시 현재 직면한 문제를 해결하기 위해 블록체인 기술을 도입하는 시도가 나타나고 있으며, MedRec, GemHealth, Health Bank, MediBloc과 같은 기업들이 블록체인 기술을 접목한 다양한 개인 건강 기록 시스템을 개발 중이거나 서비스를 시작하였다[2]. 블록체인을 접목한 의료정보관리 플랫폼은 Off-Chain 형태로 블록체인 기술을 사용하여 개인 건강 기록을 관리하고 있다. <Table 1>은 딜로이트의 보고서에서 On-Chain과 Off-Chain을 비교한 내용이다. Off-Chain 형태는 기존 의료기관의 데이터베이스를 그대로 활용하되 블록체인 상에 기존 데이터베이스의 데이터 유형과 접근 경로, 접근 내역 등을 기록하여 관리하는 방식이다[10, 12].

〈Table 1〉 Classification of How to Use Blockchain

	On-Chain Data	Off-Chain Data
Data Type	• Standardized data fields containing summary information in text form (e.g. age, gender)	• Expansive medical details (e.g. notes) and abstract data types (e.g. MRI images, human genome)
Pros	• Data is immediately visible and ingestible to all connected organizations, making blockchain the single source of truth	• Storage of any format and size of data
Cons	• Constrained in the type and size of data that can be stored	• Data is not immediately visible or ingestible, requiring access to each health care organization's source system for each record • Requires Off-Chain micro-services and additional integration layers • Potential for information decay on the blockchain

블록체인 기술의 접목은 기존 개인 건강 기록 시스템의 문제점인 데이터 통합의 어려움과 정보 처리자간 표준의 불일치, 데이터 위·변조의 위험성, 데이터 보안의 위험성, 정보의 활용도 미비 등의 문제를 해결해 주는 듯 보인다. 하지만 아직 해결되지 않은 문제점과 블록체인 도입으로 인해 새롭게 발생할 수 있는 문제점이 존재한다. 첫째, Off-Chain 방식의 블록체인 사용은 앵커링 기술을 통해 기존 시스템의 위·변조를 감지할 수는 있으나 본래의 값을 복원할 수는 없다. 복원을 위해서는 별도의 백업 서버를 구축해야 한다. 둘째, 블록체인 시스템 자체의 보안 문제가 계속적으로 대두되고 있다. 블록체인의 내용은 네트워크의 모든 참여자가 공유하기 때문에 블록체인의 보안에 문제가 생길 경우 데이터의 대량 유출이 발생할 수 있다. 셋째, 블록 채굴을 위한 과도한 비용 지출이 발생한다. 블록체인 특유의 작업 증명 기법은 많은 양의 전산 장비와 전력 소모를 요구한다. 블록체인 도입으로 인하여 중앙 시스템의 부담은 감소할지 모르지만 전체 시스템의 비용을 고려했을 때 오히려 비용의 증가가 발생할 수 있다. 넷째, 개인 건강 정보의 완전한 소유가 아니다. 블록체인을 이용한 시스템의 데이터는 나의 기기에 존재하는 것이 아니며, 기존의 중앙 시스템 혹은 미지의 노드들에 저장되어 있다. 다섯째, 개인키 분실로 인한 데이터의 유실의 위험이 크다. 블록체인 시스템은 보안을 위해 최초 발행한 개인키의 보관이 중요하다. 이를 분실할 경우 블록체인 상의 나의 모든 데이터를 찾을 수 없게 된다.

2.3 블록체인 기반 건강 정보 시스템 관련 법제도 분석

블록체인 기반의 건강 정보 시스템의 구현 및 사용은 앞서 말한 기술적 문제뿐만 아니라 해결해야할 법적 문제도 함께 제기되고 있다.

국내 개인정보 보호법 제15조(개인정보의 수집·이용)에 의하면 개인정보처리자는 정보주체의 동의를 얻어 개인정보를 수집할 수 있으며, 정보의 이용 목적 등을 정보주체에게 고지하여 해당 목적을 위해 정보를 처리할 수 있다. 여기서 개인정보처리자란 업무를 목적으로

〈Table 2〉 Data Storage and User Rights by Health Information Management Systems

	Hospital Information System	Personal Health Record System	Blockchain based Health Record System	Suggested system
Data Storage	Each medical institution	PHR Service Provider	Each medical institution & Blockchain Network	Each medical institution & Personal Device
User Rights	Reading	Reading & Recording	Reading & Recording & Manage Authority	Reading & Recording & Manage Authority

개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다. 동법 제23조(민감정보의 처리 제한)에서 역시 개인정보처리자는 건강 정보를 포함한 민감정보에 대해 정보주체에게 민감정보에 대한 별도의 동의를 얻는 경우에 한하여 수집 및 처리할 수 있다고 명시하고 있다. 또한, 동법 제17조(개인정보의 제공)와 제18조(개인정보의 목적 외 이용·제공 제한)에 따르면 개인정보처리자는 정보주체로부터 동의를 얻는 다면 제3자에게 해당 정보주체의 개인정보를 제공할 수 있도록 명시하고 있다[8].

하지만, 의료법 제21조(기록 열람 등)와 제21조의2(진료기록의 송부 등)에서는 본인 혹은 환자의 가족, 해당 법에서 지정한 공공기관, 해당 환자의 응급의료를 수행하는 타 의료기관, 환자 혹은 가족의 동의를 얻은 타 의료기관에 한하여 정보를 제공할 수 있도록 명시하고 있으며, 약사법 제30조(조제기록부)에 의하면 환자의 조제기록부 역시 본인 및 법정대리인, 법에서 지정한 공공기관을 제외하고는 정보를 열람할 수 없도록 되어 있다. 그 외에도 생명윤리 및 안전에 관한 법률, 인체조직안전 및 관리 등에 관한 법률에서 역시 개인의 건강 정보를 제3자에게 제공할 수 없도록 명시하고 있다[7, 9].

이와 같이 현행법상 블록체인 기반의 건강 정보 시스템의 구현 및 사용은 많은 제약이 따른다. Off-Chain 방식의 시스템이 개인의 건강 정보를 블록체인이 아닌 의료 기관에 보관하기 때문에 위법 사항이 아니라고 판단될 수도 있지만 해당 정보에 접근할 수 있는 경로 및 권한이 앞서 말한 기술적 문제로 인하여 유출될 우려가 있으며, 이에 따라 의료법 시행령 제10조의4(진료기록전송지원시스템 보유 정보의 안전성 확보 조치)에 위배된다고 해석될 수 있다[6].

이에 본 연구자는 <Table 2>과 같이 정보의 저장 및 관리의 주체를 의료기관 혹은 제3자 개인정보처리자가 아닌 정보주체가 직접 자신의 건강 정보를 저장하고 관리하는 방안을 제안하고자 한다. 개인정보보호법, 의료법, 약사법 등 모든 법령에서 정보주체가 자신의 개인 건강 정보의 열람 및 사본의 발부는 정보주체의 기본적 권리로 보고 있다. 제안 프레임워크는 정보주체가 직접 자신의 건강 정보를 저장 및 관리하며 건강 정보를 취급할 수 있는 기관들과의 네트워크를 구성하고, 암호화된 P2P 방식으로 데이터를 공유한다. 그 외에 데이터의 검증 및 보안 유지를 위한 기술적 방법은 3장에서 서술하였다.

3. 분산 원장 기술 기반의 개인 건강 데이터 관리 프레임워크

본 장에서는 제안 프레임워크의 설계 목표와 설계를 위해 참고한 기술, 설계된 프레임워크의 내용, 제안 프레임워크의 적용 시나리오를 서술하였다.

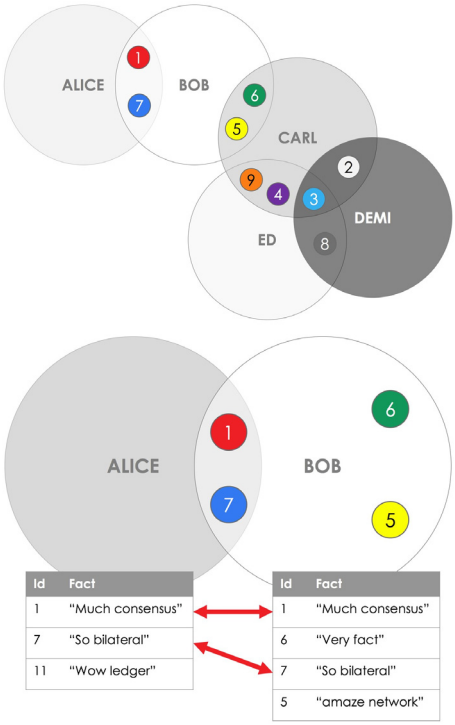
3.1 프레임워크 설계 목표

제안 프레임워크의 설계 목표는 다음과 같다. 첫째, 정보주체가 건강 정보를 직접 보유할 수 있도록 한다. 이를 위해 개인의 모바일 장치에 정보를 저장할 수 있도록 한다. 둘째, 정보의 신뢰성과 무결성을 확보한다. 셋째, 정보주체와 건강 정보 취급 기관들 간의 네트워크를 구성한다. 넷째, 구성원 간 안전한 데이터의 송수신이 가능하게 한다. 다섯째, 데이터의 위·변조를 방지하고 손실된 데이터에 대한 복구가 가능하도록 한다. 여섯째, 건강 정보 활용도 증진을 위해 네트워크 구성원 간 검색이 가능하도록 한다.

3.2 프레임워크 참조 기술

제안 프레임워크의 설계 목표를 달성하기 위해 기존의 시스템들을 분석한 결과 컨소시엄 블록체인 유형 중 하나인 R3 Corda가 가장 적합한 시스템으로 판단되어 Corda의 기본적 구조를 참고하여 프레임워크 설계에 반영하였다.

<Figure 1>와 같이 Corda는 기존의 블록체인 시스템과 달리 원장을 네트워크의 모든 참여자가 공유하지 않고, 데이터의 생성에 참여하는 노드들만 데이터를 공유한다. Corda의 데이터 분산 방법은 본 연구의 첫 번째 목적인 정보주체의 직접적 데이터 보유를 위한 시스템을 구현하기 위해 매우 적합한 형태이다. 또한 기존 블록체인의 합의에 의한 데이터 검증 방식과 달리 네트워크 참여자의 부담을 최소화하는 방식을 채택하였다[14].



〈Figure 1〉 R3 Corda Ledger Concept

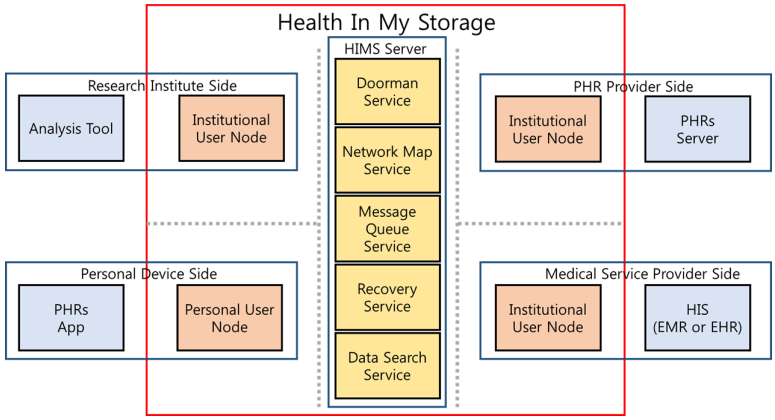
하지만, Corda 시스템으로 제안 시스템의 모든 목표를 달성하기에는 한계점이 있다. 첫째, Corda는 네트워크 참여자 간 데이터 검색을 허용하지 않는다. 둘째, 노드 자체가 손상 혹은 삭제될 경우 노드를 복구할 수 없다. 셋째, 고정된 IP주소의 필요, Server 기능의 탑재 등 개인의 모바일 장치에 사용하기에 적합하지 않다.

이에 본 제안시스템의 목표를 달성하기 위해 R3 Corda 시스템의 구조를 기반으로 자체 프레임워크를 설계하였으며, 각 노드에 불필요한 기능을 삭제하고 목표 달성을 위해 필요한 추가 기능을 설계하였다.

3.3 프레임워크 설계

분산 원장 기반의 개인 주도적 건강 정보 관리 시스템(Health In My Storage : HIMS)을 설계하기 위해 기본적인 시스템 구성요소를 <Figure 2>와 같이 설계하였다.

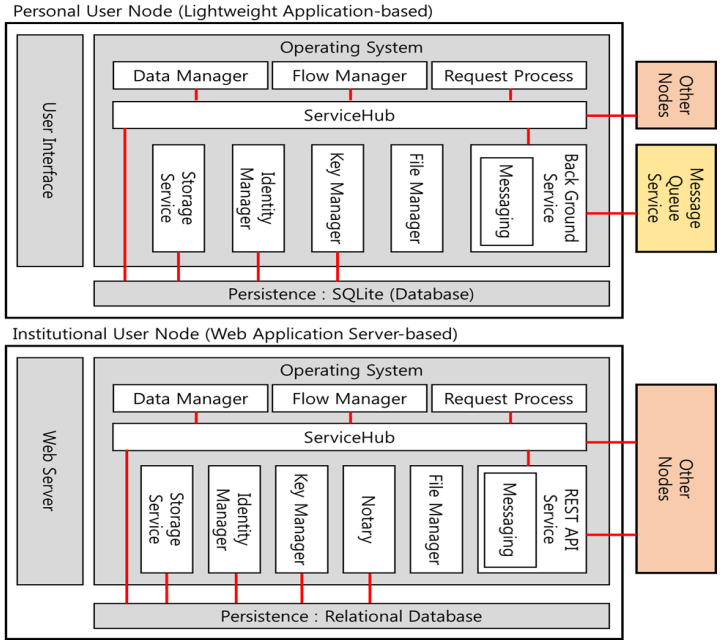
시스템 구성 요소 중 첫 번째 요소는 시스템에 참여하는 각 노드에 대한 등록 및 인증을 하는 Doorman Service 이다. 제안된 시스템의 인증 서비스는 블록체인의 개인키 분실 문제를 해결하기 위해 블록체인 시스템 보다는 레거시 시스템에 가깝게 설계하였다. Doorman Service는 사용자가 지정한 특정 값을 토대로 개인키와 공개키를 생성하여 개인키는 각 노드에 저장하도록 하고 공개키는 중앙 서버에 저장하여 노드 간 통신에 사용할 수 있도록 제공한다. 사용자가 개인키를 분실한 경우 사용자 지정 값을 토대로 개인키와 공개키를 다시 재현할 수 있도록 한다. 두 번째 구성요소인 Network Map Service는 시스템에 참여하는 각 노드에 접근할 수 있는 경로를 제공하는 서비스이다. 세 번째 구성요소인 Message Queue Service는 개인 사용자를 위한 메시지 전송 서비스이다. 설계에 참고한 R3 Corda 플랫폼은 모든 노드가 고정 IP를 보유하는 것을 전제로 한다. 하지만 모든 개인 사용자가 고정 IP를 소유하는 것이 어렵기 때문에 개인 사용자 노드에 한하여 IP 주소 기반의 접근이 아닌 Message Queue Service에 의한 접근을 제공한다. 이를 통해 스마트폰과 같은 개인 디바이스가 하나의 노드로 구성될 수 있도록 한다. 또한 노드의 상태 이상으로 수신에 실패한 메시지를 저장하고 노드가 복구되면 수신할 수 있도록 지원한다. 개인 사용자 노드를 제외한 의료 서비스 제공자, 개인 건강 기록 시스템 제공자, 연구기관은 전체적인 시스템의 운영을 위해 고정 IP의 사용을 전제조건으로 한다. 네 번째 구성요



〈Figure 2〉 Components of Health Data Management System based on Distributed Ledger

소인 Recovery Service는 노드 중 일부가 장애로 인한 데이터 손실이 발생하였을 경우를 대비한 요소이다. 이 서비스는 장애가 발생한 노드의 복구 요청을 받아 브로드 캐스트로 네트워크에 연결된 모든 노드에서 장애가 발생한 노드와 관련된 데이터를 수집하고, 복구 작업을 수행한다. 다섯 번째 구성요소인 Data Search Service는 연구기관을 위한 서비스이다. 이 서비스는 연구기관의 노드가 연구 활동을 위해 전체 노드의 데이터 중 연구에 필요한 데이터를 가진 노드를 검색하는 기능이다. 단 제공되는 데이터는 사용자의 개인정보를 인지할 수 없도록 비식별화하고, 데이터 값을 제외한 데이터의 구성만을 제공한다. 연구 기관은 제공 받은 데이터의 구성을 검토하여 원하는 노드와 데이터 거래를 진행할 수 있도록 지원한다. 마지막 구성요소인 Node는 각각의 말단 사용자를 위한 구성요소로 각 노드의 데이터, 데이터의 흐름, 메시지 송·수신 등의 기능을 수행한다. 노드는 크게 개인 사용자를 위한 노드와 기관을 위한 노드로 나뉘며 이는 각 노드 사용자의 특성에 맞춰 가용한 자원을 사용하여 전체 시스템 운영에 기여하도록 한다.

<Figure 3>의 상단은 개인 사용자를 위한 노드 구성이다. 개인 사용자는 스마트폰을 기본 디바이스로 사용하는 것으로 하며, 이를 위해 노드의 구성 서비스를 최소화 하였다. 개인 사용자 노드의 기본적인 기능은 HIMS Server의 Message Queue Service에서 메시지를 수신하여 해당 요청을 처리하거나 새로운 데이터를 생성하는 것과 Flow Manager를 통해 다른 노드와 원장 거래를 진행하는 것이다. 개인 사용자 노드의 모든 메시지 송신은 JSON 형태로 REST 통신 방식으로 이루어지며, 수신은 Firebase platform에서 제공하는 Cloud Messaging 서비



〈Figure 3〉 Node Application

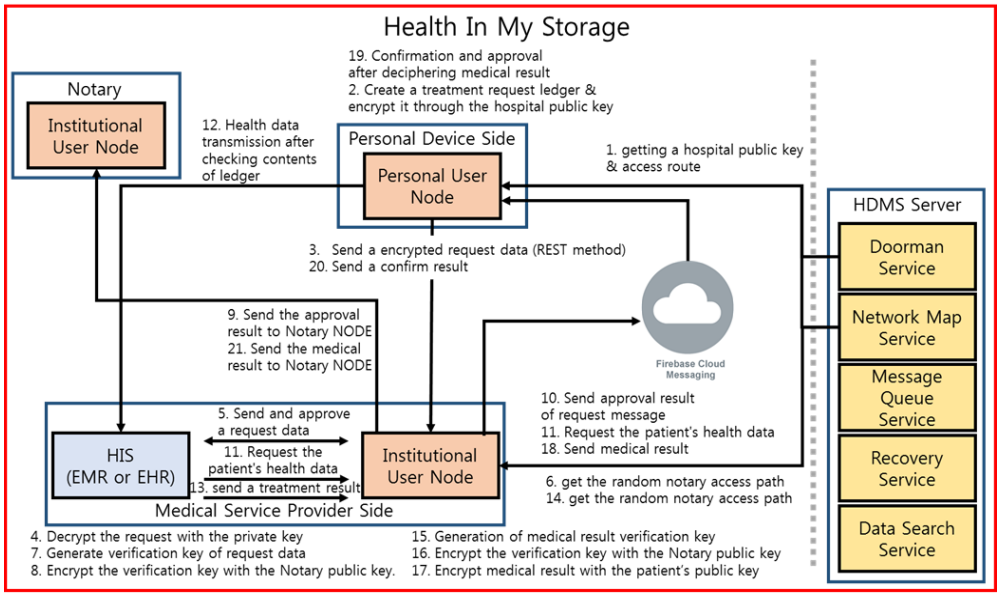
스를 통해 이루어진다. 이는 개인 사용자 노드의 모바일 디바이스에는 수신기능을 수행할 Server 시스템을 탑재할 수 없기 때문이다. 그리고 Firebase Cloud Messaging 서비스를 사용하면 네트워크의 모든 개인 사용자에게 일괄적 메시지 발송이 가능해진다. 이것은 HIMS의 Data Search Service, Recovery Service를 위한 기능으로서의 역할을 한다. File Manager는 건강 정보 중 이미지, 동영상, 음성 자료를 저장하기 위한 기능으로써, 모바일 디바이스의 특성에 맞게 자료를 보관 및 관리한다. 모바일 디바이스는 항상 대용량의 자료를 송·수신 하는 것에 한계가 있기 때문에 File Manager는 송·수신 요청에 대하여 대용량 자료를 송·수신할 수 있는 상태일 때 처리할 수 있도록 요청의 수행 시점을 확인하고 처리한다.

<Figure 3>의 하단은 기관 사용자 노드의 구성이다. PHR 서비스 제공자, 의료 서비스 제공자, 연구 기관이 이에 해당하며, 기관 사용자 노드는 고정 IP 기반의 웹서버의 형태로 구성된다. 기본적인 요청 처리와 데이터 생성 및 생성된 데이터의 원장 거래는 개인 사용자 노드와 동일하며, 메시지를 수신하는 서비스를 REST API 형태로 구성하여 Message Queue Service를 거치지 않고 메시지를 수신할 수 있도록 한다. 이는 HIMS Server의 부담을 줄이기 위함이며, 데이터의 흐름을 분산시킴으로써 전체적인 시스템의 속도를 향상시킬 수 있다. 기관 사용자 노드에는 개인 사용자 노드에 없는 하나의 구성이 추가된다. 추가된 구성은 Notary 서비스이다. 네트워크에 참여하는 모든 기관 사용자가 다른 노드들 간의 원장 거래의 공증인이 되는 것이다. 이때 모든 노드가 공증인이 되는 것은 아니며 거래 참여자의 수에 따라 적정수의 공증인을 임의로 선택하여 지정한다. 공증인을 통해 네트워크 내의 데이터 위·변조 및 부정을 방지한다. 그리고 File Manager 서비스의 기능이 개인 사용자 노드의 기능과는 다르게 구성된다. 기관 사용자 노드의 File Manager는 기관의 기존 파일 관리 시스템에 접근할 수 있는 권한을 관리하고, 기존 시스템의 보안을 유지하기 위해 외부의 요청에 따라 기존 시스템의 파일 데이터를 복사하여 요청을 처리하도록 한다. 이를 통해 기존 시스템의 모든 파일 데이터가 외부로 유출되는 것을 방지한다.

3.4 적용 시나리오

3.4.1 진료 요청 및 진료 내역 저장 시나리오

<Figure 4>는 개인 사용자인 환자가 특정 병원에 진료 요청을 하고 진료 결과 데이터를 병원 노드와 개인 사용자 노드에 각각 저장하는 가상 상황을 도식화한 것이다. 환자는 HIMS의 서비스에서 특정 병원의 공개키와 접속 경로를 획득하고 진료 요청 원장에 진료 요청 내용과 자신의 아이디 및 공개키를 병원의 공개키로 암호화하여 병원 노드에 전송한다. 병원 노드는 원장을 개인키로 복호화하고, 내용을 확인 후 승인한다. 승인 내역은 HIMS를 통해 개인 노드로 전송되고 이렇게 진료 요청 원장이 완성된다. 완성된 원장은 임의 선택된 공증인 노드에게 원장의 검증키를 전송한다. 병원 노드는 연결된 병원 정보 시스템에 원장의 내용을 공유하고 원장의 내용을 토대로 환자 노드에 환자의 건강 데이터를 요청한다. 환자의 노드는 병원 정보 시스템의 요청 내용과 원장의 내용을 대조하여 올바른 요청으로 판단될 때 자신의 건강 데이터

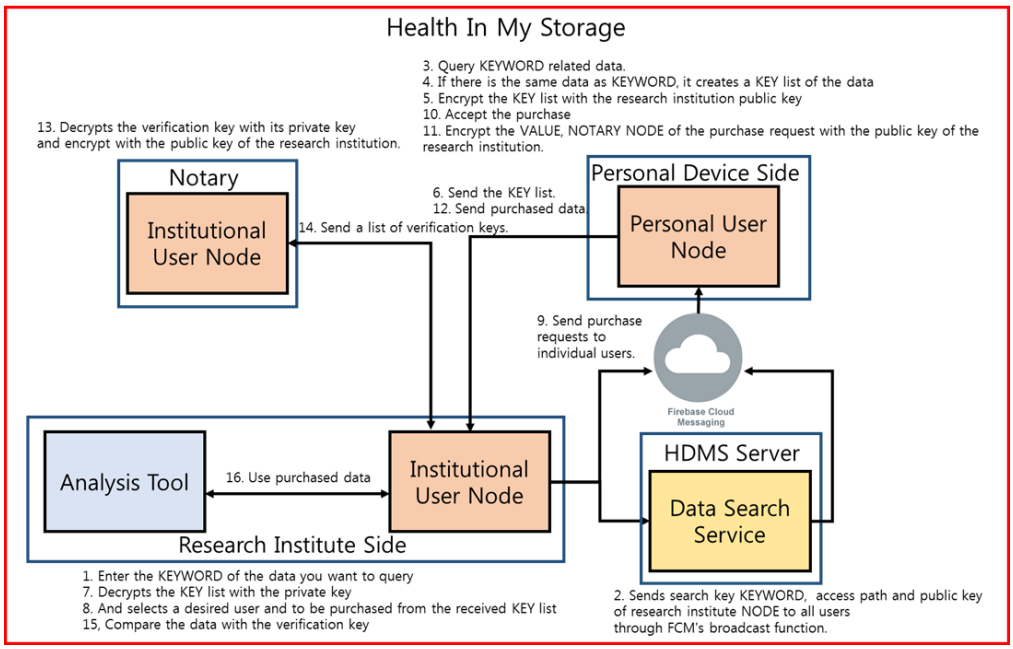


〈Figure 4〉 Scenario of Hospital Treatment

를 송신한다. 의사는 수신된 건강 데이터를 참고하여 고품질의 의료서비스를 제공할 수 있게 되고, 진료의 결과를 다시 진료 결과 원장으로 작성하여 환자 노드에 전송한다. 마지막으로 환자가 노드의 데이터를 확인 후 최종 승인하여 하나의 건강 데이터 원장이 생성된다. 건강 데이터 원장 역시 생성 후 검증키를 임의의 공증인 노드에 전송되어 저장된다.

3.4.2 개인 건강 데이터 거래 시나리오

<Figure 5>는 개인건강 데이터 거래 시나리오의 흐름을 도식화 한 것이다. 개인 건강 데이터 거래의 시작은 연구 기관에 의해 시작된다. 연구 기관에서 HIMS의 Data Search Service에 원하는 데이터의 검색을 요청한다. Data Search Service는 해당 요청 내용을 모든 개인 사용자 노드에 송신한다. 개인 사용자 노드는 요청 데이터를 포함하고 있는 노드들을 비식별화하고, 데이터의 값을 제외한 데이터의 구조를 제공한다. 연구 기관은 검색 결과 중 원하는 노드를 선택하여 거래를 요청한다. 이때 거래 요청 데이터의 흐름은 앞에서 본 진료 요청의 흐름과 같다. 개인 사용자는 요청을 확인하고 거래를 원할 시 승인한다. 거래의 내역은 데이터 생성에 참여한 의료기관 혹은 개인 건강 기록 서비스 제공자에게 공지되고, 해당 건강 데이터를 보유하고 있는 공증인 노드와 대조하여 데이터를 검증한 후 연구 기관에 전송된다. 이때 연구 기관이 지불한 데이터 구매 대금은 개인 사용자와 데이터 생성에 참여한 노드(의료 서비스 제공자 혹은 개인 건강 기록 서비스 제공자), 데이터의 신뢰성을 확보하는데 일조한 공증인 노드가 일정 비율로 분배한다. 연구 기관은 데이터를 활용하여 연구를 진행한 후 해당 데이터의 가치를 평가한다. 평가 결과는 데이터 생성에 참여한 노드들의 신뢰도로 평가 지표로 사용된다.



〈Figure 5〉 Scenario Of Health Information Trading

3.5 제안 프레임워크의 기대효과

본 연구에서 제안하는 분산 원장 기반의 개인 건강 데이터 관리 프레임워크는 기존 개인 건강 기록 시스템의 문제점과 블록체인을 도입한 개인 건강 기록 시스템의 문제점을 대체로 보완할 수 있을 것으로 예상한다. 특히 기존의 시스템들은 데이터의 소유권이 온전히 개인에게 주어지지 않는 반면 본 프레임워크는 정보주체가 자신의 데이터를 직접 소유한다. 이로 인해 개인은 직접적으로 자신의 데이터에 대한 활용 권한, 이력 관리 등을 할 수 있다. 또한 개인 사용자는 네트워크의 직접 참여자가 됨으로서 건강 정보의 활용으로 발생하는 이익을 공유할 수 있으며, 이를 통해 건강 정보의 활용도를 증진시킬 수 있다. 이로 인하여 국민 건강 증진과 의료 기술의 발전을 이룰 수 있을 것이다. 그리고 기존 시스템은 병원 혹은 블록체인 시스템에 문제가 발생하였을 때 정보의 손실이 발생할 수 있지만 제안된 시스템은 정보주체가 데이터를 직접 보관함으로써 건강 데이터를 온전히 보전할 수 있다.

4. 연구 요약 및 향후 연구 계획

본 연구는 개인의 건강 데이터를 온전히 개인의 소유로 하며, 블록체인 도입으로 인한 전체 시스템의 부담을 피하고, 스마트폰에서 사용가능한 가벼운 노드의 구성으로 개인이 쉽게 사용할 수 있는 시스템을 제안하였다. 전체 시스템의 효율성을 위해 가용한 자원을 최대한 활용하되 사용된 노드의 자원에 대한 금전적 보상을 제공함으로써 전체 시스템을 유지할 수

있도록 하였다. 건강 데이터를 정보 주체가 소유하고 공유할 수 있는 네트워크를 구축함으로써 건강 정보의 활용도를 향상 시키며, 공중 보건의 증진과 의료 산업의 발전을 도모한다.

하지만 본 시스템의 개인 노드를 개인 모바일 디바이스를 사용함에 있어 장치 자체의 보안성 문제로 인한 우려가 있다. 그러나 기존의 중앙 집중식 개인 건강 기록 시스템이나 블록체인 기반의 개인 건강 기록 시스템의 경우 보안 문제 발생 시 대규모의 데이터가 유실되는 반면 본 제안 시스템은 네트워크의 모든 참여자를 해킹한다는 것이 사실상 불가능에 가깝기 때문에 데이터 유실의 문제를 최소화할 수 있을 것이라 예상한다.

추후 연구에서는 아직 확립하지 못한 원장 데이터의 구성, 데이터 흐름의 로직을 설계하고, 더욱 다양한 적용 시나리오를 토대로 설계를 고도화하여 실제 운용 가능한 시스템을 구현할 것이다. 시스템의 구현을 위해 Firebase 시스템, 암호화 기법, 파일 관리 기법, 데이터 통신 기법 등을 사용할 것이다.

References

[1] Healthcare Information Management and Systems Society, “HIMSS personal health records definition and position statement,” http://www.himss.org/content/files/phrdefinition071707.pdf, 2009.

[2] Jeon, J. and Kim, Y., “Case Study of Medical Record Management Platform using Block Chain,” Korea Software Congress 2019, 2018.

[3] Kim, D. S., “Current Status and Implications of Distributed ledger Technology and Digital Currency”, Bank of Korea Report, 2016.

[4] Kim, E., “A Study for the Innovativeness of Blockchain,” The Journal of Society for e-Business Studies, Vol. 23, No. 3, pp. 173-187, 2018.

[5] Kim, H. S., “New Growth Engine and Inclusive Growth in the 4th Industrial Revolution,” The Korean Economic Forum, pp. 59-92, 2018.

[6] Korea Ministry of Government Legislation, “Enforcement Decree of the Medical Service Act,” 2019.

[7] Korea Ministry of Government Legislation, “Medical Service Act,” 2019.

[8] Korea Ministry of Government Legislation, “Personal Information Protection Act,” 2017.

[9] Korea Ministry of Government Legislation, “Pharmaceutical Affairs Act,” 2019.

[10] Krawiec, R. J., Housman, D., White, M., Filipova, M., Quarre, F., Barr, D., Nesbitt, A., Fedosova, K., Killmeyer, J., Israel, A., and Tsai, L., “Blockchain: Opportunities for Health Care,” https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-blockchain-opportunities-for-health-care.pdf, 2016.

[11] Lee, K. S., “Core Technology Trends Leading the Fourth Industrial Revolution,” Kessia Issue Report, Korea Embedded

Software and System Industry Association, 2017.

[12] Linn, L. A. and Koo, M. B., “Blockchain for health data and its potential use in health IT and health care related research,” ONC/NIST Use of Blockchain for Healthcare and Research Workshop, Gaithersburg, Maryland, United States: ONC/NIST, 2016.

[13] Park, S., “Analysis of the main themes of the Fourth Industrial Revolution,” Statistics Korea Report, 2017.

[14] R3, “R3 Corda Development Documentation Version 4,” https://docs.corda .net/releases/release-V4.0/, 2019.

[15] Tang, P. C., Ash, J. S., Bates, D. W., Overhage, J. M., and Sands, D. Z., “Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption,” Journal of the American Medical Informatics Association, Vol. 13, No. 2, pp. 121-126, 2006.

저 자 소 개

문준호 (E-mail: jhmoon@soongsil.ac.kr)
2012년 숭실대학교 산업정보시스템공학과 졸업 (학사)
2014년 숭실대학교 산업정보시스템공학과 졸업 (석사)
2015년~현재 숭실대학교 산업정보시스템공학과 재학 (박사)
관심분야 BPM, MIS, 데이터베이스, 분산 원장, e-Health

김동수 (E-mail: dskim@ssu.ac.kr)
1994년 서울대학교 산업공학과 (학사)
1996년 서울대학교 산업공학과 (석사)
2001년 서울대학교 산업공학과 (박사)
2001년~2003년 한국전산원 전자거래연구부 e-Biz 표준팀장
2003년~2006년 가톨릭대학교 의료경영대학원 전임강사, 조교수
2006년~현재 숭실대학교 산업·정보시스템공학과 교수
관심분야 BPM, 프로세스 마이닝, O2O, e-Health, 정보보호