사물인터넷 환경에서 허가형 블록체인 기반 민감한 센싱 데이터 공유 시스템

강길욱[1,2], 김영갑[1,2,†]
[1]세종대학교 정보보호학과
[2]세종대학교 지능형드론융합전공
giluk1027@sju.ac.kr, alwaysgabi@sejong.ac.kr

Private Blockchain-based Sensitive Sensing Data Sharing System in IoT Environment

Giluk Kang[*], Young-Gab Kim[*,†]
[*]Dept. of Computer and Information Security, and Convergence Engineering for Intelligent Drone, Sejong University

요 약

사물인터넷 기기들의 빠른 발전과 보급으로 인해 다양한 센서들부터 센싱 데이터가 수집되고 있다. 이에 따라, 많은 센싱 데이터 중 헬스케어 데이터를 기반으로 맞춤형 건강 서비스를 제공하는 사물인터넷 기반 헬스케어 분야가 발전하고 있다. 하지만, 사물인터넷 기기를 통해 수집되는 헬스케어 데이터는 민감한 데이터를 포함하기 때문에 헬스케어 데이터의 공유가 이뤄질 경우, 적절한 사용자만이 헬스케어 데이터를 사용할 수 있도록 해야 한다. 따라서, 본 논문은 사물인터넷 환경에서 속성기반암호화를 통해 적절한 사용자만이 데이터를 사용할 수 있도록 하고, 블록체인의 분산원장을 통해 데이터의 무결성과 책임추적성을 보장하는 민감한 센싱 데이터 공유 시스템을 제안하고자 한다.

1. 서론

최근 사물인터넷(Internet of Things; IoT)은 4차 산업혁명의 핵심 원동력으로서 다양한 분야에 응용되고 융합되면서 새로운 서비스를 창출하고 있다.[1] 이에 일상생활에도 다양한 IoT기기들이 급속도로 보급되었고, 많은 센서들로부터 센싱 데이터들이 수집되기 시작했다. 특히, 많은 병원에서 이러한 센싱 데이터 중 헬스케어와 관련된 데이터들을 기반으로 개인의 건강 향상을 위한 맞춤형 건강 서비스를 제공하려고 시도하고 있으며[2], 코로나바이러스감염증-19(COVID-19)의 확산으로 인해 사람 간 접촉을 최소화하려는 시도가 이뤄짐에 따라 IoT 기기들로부터 수집한 헬스케어 데이터를 토대로 원격진료 및 건강 서비스 제공해주는 비대면 헬스케어 기술의 관심도 급격히 증가하고 있다.[3]

Ericsson에 따르면 5G와 결합한 디지털 헬스케어의 시장 규모는 2026년까지 760억 달러로 성장할 것으로 예측했으며[4], 미국에서도 이에 발맞춰 헬스케어 분야의 규제 완화 및 개선을 지속함에 따라 IT 기업인 Amazon, Apple, Microsoft 등이 IoT 기반 헬스케어 분야에 적극적인 투자를 진행하고 있어 성장속도는 더욱 빨라질 것으로 기대된다. 하지만, 국내에서는 개인정보보호법과 같은 법적규제로 인해 민간기관이 디지털 헬스케어 시장을 주도하지 못하고 있으며, IoT기기들이 사용자의 일상에 깊숙이 들어와 민감한 정보를 포함한 데이터를 수집함에 따라 개인정보 유출과 같은 여러 위협들이 있어 수집되는 헬스케어 데이터의 안전한 공유는 필수적으로 요구되고 있다. 또한, 최근 들어 많은 연구들에서 헬스케어 데이터의 보안을 고려하고 있지만, 사후 관리를 위한 책임추적성과 부인방지에 대한 고려는 매우 부족하다. 이에 따라, 본 논문에서는 사물인터넷 환경에서 속성기반 암호화를 통해 적절한 속성조합을 가진 사용자만이 민감한 센싱 데이터를 복호화 할 수 있도록 하여 세밀한 접근제어 및 안전한 공유가 이뤄질 수 있도록 하고, 허가형 블록체인을 통해 데이터의 무결성과 책임추적성이 보장되는 민감한 센싱 데이터 공유 시스템을 제안하고자 한다. 본 논문의 구성은 다음과 같이 구성된다. 2장에서는 기존 헬스케어 시스템과 관련된 연구들을 분석한다. 3장에서는 사물인터넷 환경에서 허가형 블록체인 기반으로 민감한 센싱 데이터인 헬스케어 데이터 공유 시스템

† 교신저자

을 제안한다. 4장에서는 제안 시스템을 관련 연구들과 비교해 평가한다. 마지막으로, 5장에서는 결론과 향후 연구에 대해 서술한다.

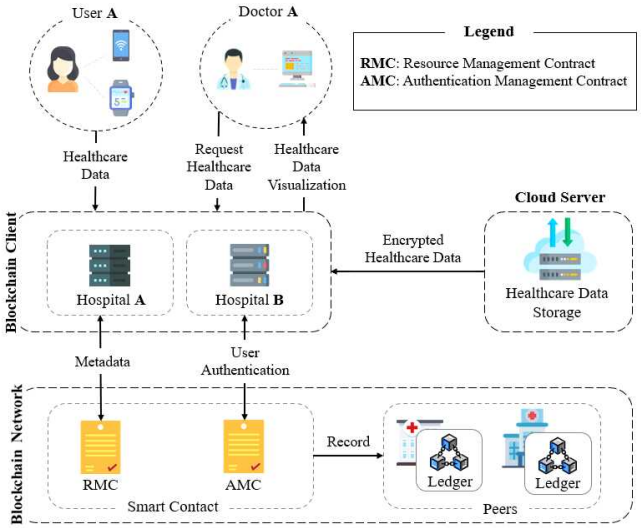
2. 관련 연구

최근 IoT기기를 이용한 헬스케어 서비스에 관심이 증가함에 따라 다양한 정보통신기술과 결합한 헬스케어 기술 연구가 활발히 진행되고 있다. 김영규 외[5]는 지정맥 기반 생체인증기술을 이용해 헬스케어 서비스를 제공받을 수 있는 시스템을 제안했다. 이는 시스템 인증을 수행할 수 있을 뿐만 아니라 공간제약을 받지 않아, 어디서든 헬스케어 서비스를 제공받을 수 있다. 김종혁 외[6]는 동형 암호화 기술을 이용해 헬스케어 데이터를 안전하게 공유하는 방법을 제안했다. 이는 민감한 데이터는 절대 노출되지 않으면서 데이터 연산을 할 수 있어, 데이터의 유용성이 증대되는 효과를 가져 오지만 현재 기술로는 기본적인 연산만 수행할 수 있다는 단점이 있다.

이 밖에도 금융, 물류, 보안, 공공서비스 등 다양한 분야에서 최근 들어 적용되고 있는 블록체인을 이용한 연구도 활발히 진행 중에 있다. 최예진 외[7]는 허가형 블록체인 플랫폼인 하이퍼레저 패브릭(Hyperledger Fabric)을 이용한 헬스케어 데이터 관리 및 공유 플랫폼을 제안했다. 이는 하이퍼레저 패브릭 플랫폼 내 프라이빗 데이터 기술을 이용하여 환자의 데이터를 안전하게 보호하고, 데이터 공유 시에 환자에게 일정 보상을 주도록 해 헬스케어 데이터 공유를 유도한다. Theodouli 외[8]는 헬스케어 데이터의 무결성과 제공자 익명성을 보장하고, 감사와 책임추적성을 제공하는 블록체인 기반 헬스케어 데이터 공유 시스템을 제안했다.

3. 제안 시스템

제안 시스템은 IoT 기기의 센서들을 통해 수집되는 많은 민감 센싱 데이터 중에서 헬스케어 데이터를 안전하게 공유하기 위한 시스템이다. 본 시스템이 적절히 동작하기 위해서 몇 가지 요구사항이 존재한다. 첫째, 해당 시스템을 사용하는 기관들은 블록체인 네트워크에 필수적으로 참여해야하며, 블록체인과 통신하는 블록체인 클라이언트를 구성해야 한다. 둘째, 사용자는 병원을 통해 고유 식별자를 발급받아야 하며, 해당 정보는 분산원장 내 담당 의사의 속성정보로써 기록되어야 한다. 본 장의 3.1절에서는 안전하게 헬스케어 데이터를 공유할 수 있는 시스템의 구성요소에 대해 설명하고, 3.2절에서는 시스템의 동작 방식에 대해 설명한다. 마지막으로, 3.3절에는 해당 시스템에서 불법 사용자를 탐지하는 방법에 대해 서술한다.



(그림 1) 허가형 블록체인 기반 안전한 헬스케어 데이터 공유 시스템 개요도

3.1 시스템 구성요소

제안 시스템은 IoT기기의 센서들로부터 수집된 사용자의 헬스케어 데이터가 담당 의사에게 안전하게 전달되어 맞춤형 건강 서비스를 제공 받을 수 있도록 하기 위한 허가형 블록체인 기반 헬스케어 데이터 공유 시스템이다. 이는 그림 1과 같이 사용자, 의사, 블록체인 네트워크, 블록체인 클라이언트, 클라우드 저장소로 구성되게 된다.

사용자는 헬스케어 서비스를 제공받기 위해 다양한 IoT 기기로부터 수집되는 헬스케어 데이터를 제공하는 역할이며, 의사는 시각화 된 사용자의 헬스케어 데이터를 분석해 최종적으로 사용자에게 맞춤형 건강서비스를 제공한다. 블록체인 클라이언트는 블록체인 네트워크와 직접적으로 통신할 뿐만 아니라 인접한 사용자들의 헬스케어 데이터를 정기적으로 수집해 블록체인 네트워크에 안전하게 전달하는 역할이다. 블록체인 네트워크는 제안 시스템의 핵심 구성요소로, 2개의 스마트 계약(Smart Contract)을 포함해 블록체인 네트워크 참여자(Peer), 분산원장(Ledger)으로 구성되어 있다. 2개의 스마트 계약 중 AMC(Authentication Management Contract)는 속성정보를 포함한 의사와 관련된 정보 관리를 담당하며, RMC(Resource Management Contract)는 헬스

케어 데이터의 해시 값을 포함한 메타데이터를 관리한다. 또한, 분산원장(Ledger)은 블록체인 네트워크 참여자들이 소유한 것으로, 블록체인 네트워크에서 일어나는 모든 과정과 정보를 기록해 헬스케어 데이터의 무결성과 책임추적성을 보장할 수 있도록 한다. 마지막으로, 클라우드 저장소는 암호화된 헬스케어 데이터를 안전하게 저장하는데 사용된다.

3.2 동작 방식

제안 시스템의 동작 방식은 헬스케어 데이터 저장과 헬스케어 데이터 사용으로 나눠진다. 우선, 사용자 헬스케어 데이터 저장 방식은 다음과 같다.

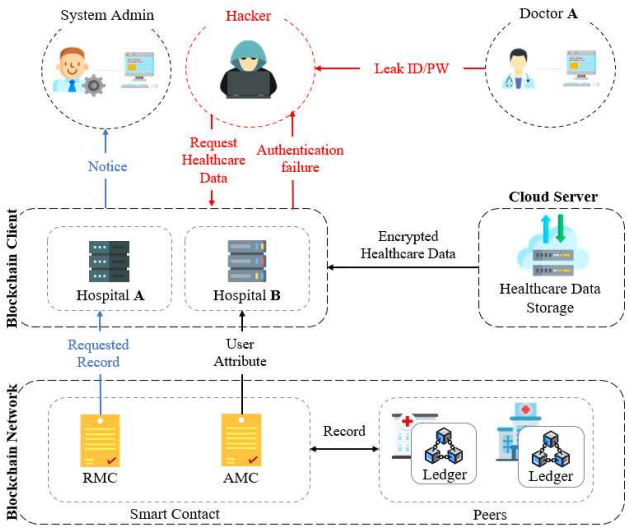
1) 사용자의 헬스케어 데이터가 암호화되어 인접한 블록체인 클라이언트에게 전달되게 된다.
2) 블록체인 클라이언트는 해당 헬스케어 데이터가 일정수준 수집되면, AMC를 호출해 담당 의사의 직급, 병원 위치 등과 같은 속성정보를 반환 받는다.
3) 블록체인 클라이언트는 담당 의사의 속성 정보를 토대로 속성기반 암호화를 수행하고, 암호화된 헬스케어 데이터를 클라우드 저장소에 전달한다.
4) 블록체인 클라이언트는 RMC를 호출해 암호화 성공/실패여부와 헬스케어 데이터의 메타데이터를 분산원장에 기록하도록 요청한다.

이러한 방식으로, 헬스케어 데이터가 저장되게 되면 담당의사는 다음과 같은 과정을 통해 헬스케어 데이터를 사용할 수 있게 된다.

1) 의사는 담당하는 사용자의 헬스케어 데이터를 사용하고자 할 경우에 블록체인 클라이언트에 접속해 로그인을 시도한다.
2) 블록체인 클라이언트는 로그인 요청 정보와 함께 AMC를 호출해 로그인 인증을 수행하고, 로그인 요청 시간 등을 기록한다.
3) AMC는 로그인 인증 결과를 반환해주고, 블록체인 클라이언트는 로그인 성공 시에 담당하는 사용자 리스트를 반환해준다.
4) 의사는 원하는 사용자의 식별자와 함께 컴퓨터에 장착된 센서들을 통해 현재 위치, 접속IP, 해시된 지문 정보 등을 같은 실시간 속성정보를 블록체인 클라이언트에 전달한다.
5) 블록체인 클라이언트는 암호화된 헬스케어 데이터를 클라우드 저장소에 요청해 전달받는다.
6) 블록체인 클라이언트는 전달받은 실시간 속성 정보와 분산원장에 저장된 속성정보를 토대로 암호화된 헬스케어 데이터의 복호화를 시도한다.
7) 블록체인 클라이언트는 복호화 결과 및 헬스케어 데이터의 해시 값 등과 함께 RMC를 호출한다.
8) RMC는 분산원장에 저장된 해시 값을 토대로 헬스케어 데이터 무결성을 검증을 수행하고, 복호화 결과와 함께 분산원장에 기록한다.
9) RMC는 헬스케어 데이터의 무결성 검증 결과를 블록체인 클라이언트에게 반환하고, 블록체인 클라이언트는 검증 결과를 토대로 헬스케어 데이터를 의사에게 시각화 해 전달한다.

3.3 불법 사용자 탐지

제안 시스템은 의사의 아이디와 비밀번호가 유출되더라도, 블록체인 내 분산원장을 통해 그림2와 같이 불법 사용자를 탐지할 뿐만 아니라 사용자의 헬스케어 데이터를 안전하게 보호할 수 있게 된다.



(그림 2) 불법 사용자 탐지 개요도

시스템의 불법 사용자 탐지 방식은 다음과 같다.

1) 불법 사용자는 불법적으로 취득한 의사의 아이디와 비밀번호를 통해 시스템에 로그인하고, 실시간 속성정보와 함께 헬스케어 데이터를 요청을 블록체인 클라이언트에 전달한다.
2) 블록체인 클라이언트는 전달받은 실시간 속성 정보와 분산원장에 저장된 속성정보를 토대로 암호화된 헬스케어 데이터의 복호화를 시도한다.
3) 올바른 속성조합이 아니기 때문에 복호화에 실패하고, 블록체인 클라이언트는 RMC를 호출해 복호화 결과를 기록하도록 한다.
4) 블록체인 클라이언트는 인증에 실패했다는 정보를 불법 사용자와 시스템 관리자에게 전달한다.

5) 시스템 관리자는 해당 정보를 토대로 불법 사용자를 판단해, 차단할 수 있게 된다.

만약, 불법사용자가 실시간 속성 정보를 위·변조해 적절한 속성조합 구성을 시도하더라도 지문, 홍채 정보와 같은 고유한 생체정보를 위·변조가 매우 어렵거나 불가능하기 때문에 헬스케어 데이터를 안전하게 보호할 수 있다.

4. 평가

2장에서 언급했듯이, 최근 들어 많은 연구들에서 헬스케어 데이터를 안전하게 공유하고자 노력하고 있지만, 헬스케어 데이터의 민감한 특징을 고려한 연구들은 부족한 상황이다.

<표 1> 제안된 시스템과 관련 연구 간의 비교

관련 연구 / 평가 기준	김영규 외[5]	김종혁 외[6]	최예진 외[7]	Theodouli 외[8]	**제안 시스템**
사용자 인증	∨				∨
안전한 공유		∨	∨	∨	∨
책임추적성			∨	∨	∨
세밀한 접근제어					∨

제안 시스템과 관련 연구들 간의 비교는 <표1>과 같다. 김영규 외[5]는 지정맥 기반 사용자 인증을 수행하지만, 헬스케어 데이터 전송 과정에서의 보안을 고려하지 않았다. 김종혁 외[6]는 동형암호화를 통해 헬스케어 데이터의 안전한 공유를 제공했지만, 민감한 데이터에 필요한 책임추적성을 전혀 고려하지 않았다. 최예진 외[7] 및 Theodouli 외[8]는 블록체인을 이용해 책임추적성을 보장하고 민감한 헬스케어 데이터 무결성 및 안전한 공유가 이뤄질 수 있도록 했지만, 세밀한 접근제어의 한계가 있으며 적절한 사용자 인증에 대한 고려가 부족했다. 하지만, 제안 시스템은 헬스케어 데이터를 사용하고자 할 때, 2번에 걸쳐 적절한 사용자 인증을 수행하며, 속성기반 암호화와 블록체인을 통해 안전한 공유, 책임추적성 그리고 세밀한 접근제어까지 달성했다.

5. 결론 및 향후 연구

일상생활에 빠르게 IoT 기기가 보급되면서, 다양한 센서들로부터 민감한 센싱 데이터가 수집되고 있다. 이에 발맞춰 민감한 센싱 데이터를 공유하기 위해 많은 보안 연구들이 진행되고 있지만 세밀한 접근제어와 사후 관리에 대한 고려가 부족하다. 따라서, 본 논문에서는 속성기반 암호화와 블록체인 기반 민감한 센싱 데이터를 안전하게 공유하는 시스템을 제안했다. 이를 통해, 적절한 속성조합에 따른 세밀한 데이터 접근제어가 수행될 뿐만 아니라, 다수의 사용자가 접근하여도 분산된 환경으로 인해 안전하게 데이터 공유 및 제공을 할 수 있다. 향후 연구는 헬스케어 데이터를 넘어서서 이기종 IoT플랫폼 간 서비스 및 장치들을 안전하게 상호운용할 수 있는 보안 상호운용 연구를 진행할 계획이다.

ACKNOWLEDGMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2021R1A2C2012635)

참고문헌

[1] 한국인터넷진흥원, “IoT 제품 • 서비스 책임강화 방안연구”, 2015.

[2] 백경화, 하은아, “모바일 기반의 디지털 헬스케어 플랫폼에 관한 연구: 스마트 웰니스를 중심으로”, 디자인학연구, 34권 1호, 101-113, 2021.

[3] 김승환, 정득영, “ICT 융합 기반의 비대면 헬스케어 기술 동향”, 한국통신학회지(정보와통신), 37권 9호, 77-84, 2020.

[4] 정보통신산업진흥원, “5G 시대, 디지털 헬스케어 동향”, 2019.

[5] 김영규, 최대영, 정상우, 백승현, 김도훈, 김대년, “지정맥 기반 인증 및 헬스케어 서비스 시스템 구현”, 한국정보기술학회논문지, 19권 1호, 147-156, 2021.

[6] 김종혁, 임효상, “공통 데이터 모델에서 동형암호화를 사용한 민감 헬스케어 정보 보호 방법”, 2020년 한국컴퓨터종합학술대회, Online, 2020, 91-93.

[7] 최예진, 김경진, “하이퍼레저 패브릭 기반의 안전한 헬스케어 데이터 관리 및 공유 플랫폼 개발 연구”, 인터넷정보학회논문지, 21권 1호, 95-102, 2020.

[8] Anastasia Theodouli, Stelios Arakliotis, Konstantinos Moschou, Konstantinos Votis, Dimitrios Tzovaras, “On the design of a Blockchain-based system to facilitate Healthcare Data Sharing”, 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications, New York, 2018, 1374-1379.