비대면 진료 시 보건의료정보의 무결성 보장을 위한 DID 기반 의료 마이데이터(MyData) 활용 기법

김희연, 임준혁, 김기형*

아주대학교

heey08@ajou.ac.kr, amigojun@ajou.ac.kr, *kkim86@ajou.ac.kr

DID-based Health MyData: Utilization of the Method to Ensure Integrity in Telehealth

Hee-Yeon Kim, Jun-Hyuk Im, Ki-Hyung Kim*

Ajou Univ.

요 약

최근 COVID-19 감염병 확산으로 인한 비대면 진료의 증가로 보건의료산업에서 생성되는 데이터 보안의 중요성이 강조되고 있다. 이에 따라 환자가 직접 본인의 데이터를 관리하고 활용하는 PHR 및 의료 마이데이터(MyData)의 필요성이 대두되면서 환자 및 의료기관의 데이터 송수신 시에 위조 및 변조를 방지하기 위한 대책이 필요할 것으로 보인다. 따라서 본 논문은 PHR인 의료 마이데이터 환경에서 비대면 진료를 할 경우 환자의 보건의료정보의 무결성을 보장하기 위한 활용 기법을 보안성 및 부인방지가 강점인 블록체인 기술을 적용한 DID를 이용하여 제안하고자 한다.

Ⅰ. 서 론

코로나바이러스감염증-19(Corona Virus Disease 19, COVID-19)의 확산으로 인해 언택트(Untact) 사회로 변화하면서 비대면 의료 시대가 열렸다[1]. 정보 통신 기술(ICT)과의 융합으로 보건의료산업이 점차 고도화 및 디지털화되면서 비대면 의료에 대한 보안성 강화 대책이 강구되고 있다. 특히 전자의무기록시스템(Electronic Medical Record, EMR) 내에 있는 환자의 성명 및 주민등록번호 등의 개인 정보와 환자의 병명 및 진단명, 질병 코드, 처치 및 투약 정보 등의 민감정보에 대한 보호 방안이 요구된다. 보건의료정보는 제3자에게 유출된다면 막대한 사회적 비용을 초래하지만 여전히 데이터 처리 및 저장 과정에서 빈번하게 유출되고 있다.

이를 해결하기 위해 기존 병원의 중앙집중형 데이터 저장 및 처리 방식을 탈피하고, 여러 의료기관에 의해 생성된 보건의료정보를 한곳에 모아 본인이 직접 관리하고 활용할 수 있는 PHR(Personal Health Record)과 의료 마이데이터(MyData)의 필요성이 제기되고 있다. 또한 환자 보건의료정보의 자기주권성에 대한 당위성이 논의되고 있지만 아직까지는 환자가 데이터를 활용함에 있어 의료 마이데이터 DB의 저장 및 처리 시 보안에 주의가 요구된다. 따라서 블록체인(Blockchain) 기술을 응용한 DID를 적용하여 보건의료정보 활용 시의 보안성을 강화하고, 환자 정보의 무결성을 보장하기 위한 기법을 제안하고자 한다. 본 논문은 2장에서 관련 연구를 제시하고 3장에서는 비대면 진료 시 DID를 기반으로 한 의료 마이데이터 활용 기법 제안 및 보안성을 분석하며 4장의 결론으로 마무리한다.

Ⅱ. 관련 연구

1. 마이데이터(MyData)

마이데이터(MyData)는 개인이 데이터에 대한 권리를 가지고 원하는 방식으로 관리 및 통제하며 정보 주체인 개인의 동의에 따라 본인 데이터를 개방하거나 활용하는 것을 의미한다. 기존 기관 중심이었던 권한 및 데이터 관리, 데이터 활용 체계에서 개인 중심으로 전환하는 새로운 패러다임으로 개인은 데이터 활용 결과를 투명하게 확인할 수 있다[2].

2. PHR(Personal Health Record)

기존 전자의무기록시스템은 의료 서비스 제공 환경에서 생성된 환자의 보건의료정보가 내부 조직 시스템 관리 기관인 병원에 저장된다. 반면, 개인건강기록(Personal Health Record, PHR)은 개인이 본인에 대한 병력 및 정보를 스스로 기록하거나 환자의 직접적인 참여로 데이터가 생성되어 투명하게 관리된다. 즉, 환자가 본인의 검사 결과 및 진료 정보를 확인하여 기록을 관리하고 건강 정보를 모니터링할 수 있는 시스템이다[3].

3. DID(Decentralized Identifier)

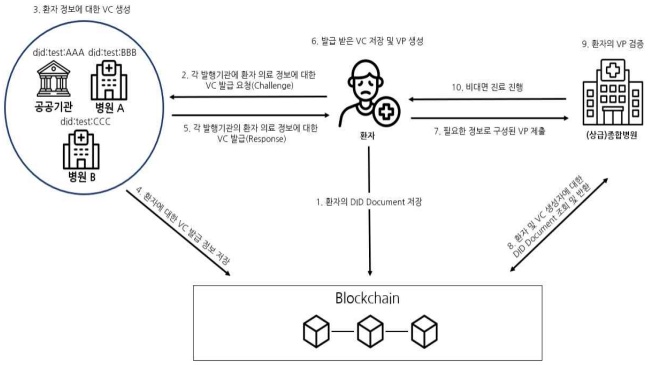
블록체인을 활용한 기술인 DID(Decentralized Identifier)는 사용자가 검증된 디지털 ID를 가질 수 있는 분산 시스템의 식별자이다[4]. 분산형 ID를 이용한 신원 검증 시스템은 검증 가능한 제3자가 신분증과 같은 자격증명을 확인하여 신원 증명을 할 수 있도록 지원한다[5]. 현재 DID 기술은 운전면허증, 공무원증 등의 모바일 신분증, 백신 예방접종 증명서, 병원 제증명 발급 서비스 등이 여러 분야에 걸쳐 활용되고 있다.

Ⅲ. 비대면 진료 시 DID 기반 의료 마이데이터 활용 기법

1. 비대면 진료 시 DID 기반 의료 마이데이터 활용 기법 제안

[그림 1]은 환자가 비대면 의료 서비스를 요청하고 제공받는 시나리오를 적용하여 DID를 기반으로 의료 마이데이터를 활용하는 기법에 대한 그림이다. 먼저 1) 환자의 DID는 DID Document 형식으로 블록체인에 저장된다. 2) 환자는 본인의 보건의료정보를 각 발행기관에 VC(Verifiable Credential) 형식으로 요청하고, 3) 공공기관, 병원 A, 병원 B는 환자 정보에 대한 내용을 VC로 생성한다. 4) 공공기관, 병원 A, 병원 B는 환자 보건의료정보에 대해 VC를 발급한 발급 정보를 분산원장에 저장하고, 5) 각 발행기관은 환자 의료 정보에 대한 VC를 환자에게 발급한다(Response).

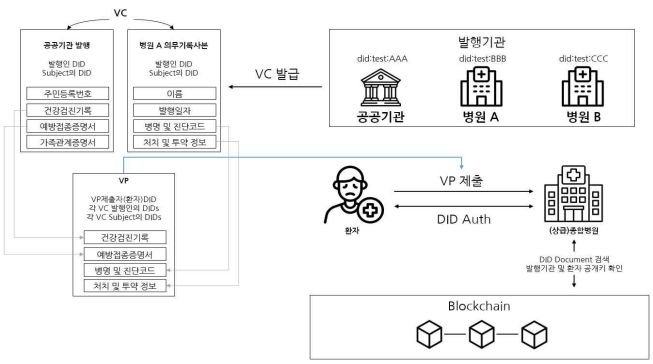
6) 환자는 각 발행기관으로부터 발급받은 VC를 저장하고 필요한 정보만 선택하여 VP(Verifiable Presentation)를 생성한다. 7) 비대면 진료를 받기 위해 필요한 정보를 선별하여 구성한 VP를 (상급)종합병원에 제출하고, 8) (상급)종합병원은 환자와 VC를 생성한 생성자인 발행기관에 대한 DID Document를 분산 원장에서 조회한 후 인증 내역을 반환한 후, 9) 환자의 VP 검증 과정을 거친다. 10) 검증과정을 통해 모든 인증이 종료되면 (상급)종합병원은 환자에게 비대면 의료 서비스를 제공한다.



〔그림 1〕 비대면 진료 시 DID를 이용한 의료 마이데이터 활용 기법

2. 비대면 진료 시 DID 기반 의료 마이데이터 활용 개념도

[그림 2]는 DID를 이용한 환자의 의료 마이데이터 활용 기법을 전체 개념도로 나타낸 그림이다. 환자는 공공기관, 이전에 진료받은 병원 A, 병원 B에서의 보건의료정보를 VC 형식으로 발급받고, 진료받고자 하는 병원인 (상급)종합병원에 VP 형식으로 환자의 보건의료정보를 제출한다. 이때 환자와 (상급)종합병원은 DID Auth 과정을 거친다. 환자는 공공기관인 건강보험공단에서 주민등록번호, 건강검진기록, 예방접종증명서, 가족관계증명서 등 공공기관에 저장된 환자 정보에 대한 내용을 VC 형식으로 발급받는다. 병원 A에서는 기존에 환자가 진료받은 내용에 대한 의무기록 사본 내의 이름, 발행일자, 병명 및 진단코드, 처치 및 투약정보에 대한 기록을 VC 형식으로 발급받는다. 이후 환자는 VC 형식으로 저장된 본인의 데이터 중에서 제공을 원하는 정보만을 선택하여 VP 형식으로 제출할 수 있다. (상급)종합병원에서 초진을 받기 위한 정보인 공공기관에서 발급받은 건강검진기록, 예방접종증명서와 병원 A에서 진료받은 내역인 병명 및 진단코드, 처치 및 투약정보에 대한 내용을 VP 형식으로 (상급)종합병원에 제출할 수 있다.



〔그림 2〕 DID 기반 환자 의료 마이데이터 활용 개념도

3. 보안성 분석

비대면 진료 시 DID 기반 환자 의료 마이데이터 활용 기법은 환자가 본인에 대한 보건의료정보 주권을 가져 정보에 대한 활용 범위 및 여부를 설정할 수 있다. 또한 환자의 데이터 송수신 시 환자 신상에 대한 내용은 최소화하고 환자 진료에 필요한 질병 정보만 전송할 수 있어 환자 개인정보를 선택적으로 제출할 수 있다는 장점이 있다. 진료받을 진료과목과 무관한 병원의 진료 기록을 선택하지 않으면 해당 정보는 공개되지 않기 때문에 환자의 프라이버시를 보장할 수 있다. 게다가 블록체인에 해당 내용을 저장 및 관리하고, DID 비대칭키 검증 방식을 이용하기 때문에 환자 데이터 송수신 과정에서의 데이터 위조 및 변조를 방지하여 무결성을 확보할 수 있다. 또한 병원마다 데이터 입력 서식이 다르기 때문에 블록체인을 이용하여 표준화하면 보건의료정보 교류의 편의성과 호환성을 향상할 수 있다. 따라서 궁극적인 비대면 의료 시스템을 보안성이 향상된 환경에서 실현할 수 있으며 데이터의 부인방지 및 무결성을 보장할 수 있다.

Ⅳ. 결 론

감염병 확산으로 인해 비대면 진료 건수가 급증하면서 비대면 의료의 본격적인 도입이 필요해지고 있다. 비대면 의료 환경에서는 환자의 모든 정보가 디지털화되어 처리되므로 보건의료정보의 유출을 방지하기 위해 가명 정보와 익명 정보 등을 사용하여 개인 정보 보호를 할 수 있지만, 블록체인 응용기술인 DID를 적용하면 비대면 시스템의 보안을 더욱 견고히 할 수 있다. 또한 본 논문에서 제안한 DID 기반 의료 마이데이터 활용 기법을 적용하면 환자가 본인의 보건의료정보에 대한 주체성을 가지고 안전하게 정보를 활용할 수 있는 신뢰성 높은 보안 환경을 갖춤으로써 향후 타 산업과의 연계를 통해 범용성이 향상될 것으로 기대된다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업과 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성지원사업과 2022년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원과 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원의 연구결과로 수행되었음.
(IITP-2021-0-01835, IITP-2023-2018-0-01396, P0008703, 2022년 산업혁신인재성장지원사업, 2021-0-00590, 대규모 노드에서 블록단위의 효율적인 거래 확정을 위한 최종성 보장 기술개발)

참 고 문 헌

[1] Dae-ha Kim. "Considerations on Untact Healthcare, Another Name for Telemedicine". The Korean Journal of Medicine (Korean J Med), vol. 95, pp.228-231, 2020. (https://doi.org/10.3904/kjm.2020.95.4.228)

[2] Lee Ki-ho. "Current Status of MyData Policy and Tasks in Health and Welfare". Health and welfare policy forum, vol. 301, pp.52-68, 2021. (https://doi.org/10.23062/2021.11.5)

[3] T. Heart, O. Ben-Assuli, and I. Shabtai, "A review of PHR, EMR and EHR integration: A more personalized healthcare and public health policy," Health Policy and Technology , vol. 6, no. 1. Elsevier BV, pp. 20 - 25, March 2017. (https://doi.org/10.1016/j.hlpt.2016.08.002)

[4] P. Szalachowski, "Password-Authenticated Decentralized Identities," IEEE Transactions on Information Forensics and Security, vol. 16. Institute of Electrical and Electronics Engineers (IEEE), pp. 4801 - 4810, 2021.

[5] I. T. Javed, F. Alharbi, B. Bellaj, T. Margaria, N. Crespi, and K. N. Qureshi, "Health-ID: A Blockchain-Based Decentralized Identity Management for Remote Healthcare," Healthcare, vol. 9, no. 6. MDPI AG, p. 712, 10-Jun-2021.