원격진료 의약품 운송에 대한 악용 방지 강화를 위한 DID 기반 운송시스템

오한수, 송해준, 최재호, 김기형*

*아주대학교

ogemini@ajou.ac.kr, young7135@ajou.ac.kr, cjh7748@ajou.ac.kr, *kkim86@ajou.ac.kr

DID-based Transport System to Enhance Anti-Abuse of Medicine Transport in Telemedicine

Han-Su Oh, Hae-Jun Song, Jae-Ho Choi, Ki-Hyung Kim*

*Ajou Univ.

요 약

정보통신 기술이 발전함에 따라 의료 분야도 원격진료를 시범적으로 운영하기 시작하였지만, 의약품 운송에 있어서는 물리적인 과정을 거치기 때문에 타인에 의한 악용 방지 대책을 따로 마련하여야 한다. 수취인을 명확히 할 수 없으며, 대리인의 수령을 방지하기 어려운 현 시스템의 문제점을 파악하여, 수취인을 명확히 할 수 있으며 VP의 속성값과 비대칭키를 통해 보안성을 강화한 DID 기반 잠금장치 시스템을 제안하였다.

Ⅰ. 서론

정보통신 기술이 발전함에 따라 산업들의 원격화가 진행되고 있다. 이에 의료산업도 코로나로 인해 원격진료 연구가 논의되고 [1], 시행하게 되며 환자가 직접 병원을 방문하지 않고 비대면 진료를 받을 수 있게 되었다. 이에 따라 처방전도 약국에 온라인으로 전송해 의약품을 운송 받는 서비스도 나타났다. 하지만 원격진료 간 개인정보 유출에 대해서는 많이 다뤄지고 있지만, 의약품 운송에 관해서는 심각성이 많이 다뤄지고 있지 않다.

의약품 운송에 있어서 오배송에는 신체적 손상이 있을 것이고, 제삼자의 획득으로 인한 악용에는 의료산업에 큰 타격을 주며, 불법시장을 형성할 수도 있다. 원격진료가 정착되기 위해서는 의약품 운송의 보안성을 빼놓을 수 없으며, 의약품 운송까지 문제가 없어야 할 것이다.

현재 택배함에 보관하거나 수취인의 문 앞까지 운송해주는 서비스도 진행 중이지만 이 방법에도 문제가 있다. 택배함의 경우 제삼자의 수령을 막기 힘들며, 수취인의 수령을 확신할 수 없다. 또한 공동현관문이 있다고 해도 개문 시에 같이 출입할 수도 있으며, 수취인이 외출한 상황에서는 물리적 탈취를 막기 힘들 것이다. 의약품 운송에 있어서 이러한 문제점들을 방지하기 위해 운송의 전 과정에 블록체인 기술을 적용하여 보안성을 향상하고, 처방전의 무결성 이점을 얻는 동시에, 오배송으로 인한 신체의 손상을 예방하는 시스템을 제안한다.

Ⅱ. 관련 연구

2.1 블록체인 및 DID

블록체인은 데이터들이 체인처럼 블록마다 이어져 있어 위변조가 불가능하며, 데이터의 무결성을 입증할 수 있는 기술이다. 해당 블록체인을 활용한 DID(Decentralized Identifier)는 중앙 기관이 필요 없는 탈중앙화된 식별자로 본인을 인증할 수 있는 DID document에 공개키와 인증 방식 등이 기재 되어 있으며, 분산원장 내에 저장되어 있다. [2]

2.2 의약품 배달앱 시스템

원격진료 처방에 의한 의약품 배달앱 시스템 운영체계 개발 논문에서는 배달앱을 통해 환자에게 의약품을 전달하는 시스템을 제안하고 있다. 원격진료가 시범적으로 시행되면서 완전한 원격 체계를 구축하고자 의약품 배달도 원격으로 운송 받는 시스템을 제안했다. [3]

2.3 블록체인을 이용한 택배 시스템

블록체인을 이용한 물품 배송 박스의 보안 시스템 및 그 방법의 특허에 있어서 해당 방식은 스마트컨트랙트를 이용하여 택배함에 공개키를 전달해놓고, 수취인은 공개키로 암호화된 주소를 개인키로 복호화해 그 주소에 공개키를 전달하여 잠금장치를 해제하는 방식을 취하고 있다. [4]

2.4 주기적인 암호 변경 및 임의의 암호 생성기 사용

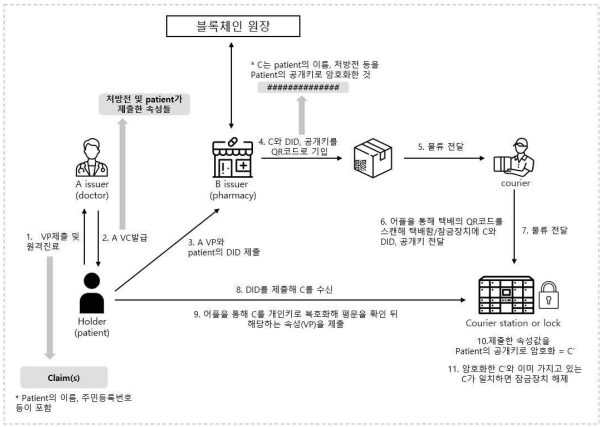
보안 전문가들은 암호를 사용할 때 암호 재사용을 지양하고, 암호 재사용은 해킹이나 암호 유출에 있어서 큰 피해를 볼 수 있기 때문에 임의 암호를 사용하도록 권장하고 있다. 하지만 사람들은 편의성과 보안성에 따라 암호를 재사용하거나 임의의 암호 생성 도구를 사용하지만, 대다수 인원이 암호를 재사용하는 방식을 채택하고 있다. [5]

Ⅲ. DID를 활용한 의약품 운송 시스템

3.1 제안 시스템

블록체인 DID를 활용하여 의약품 운송시스템의 완전한 비대면 방식을 제안하면서, 사이버공격에 대해서도 예방할 수 있는 시스템을 제안한다.

[그림 1]에서 (1) 환자는 자신이 가지고 있는 VP(Verifiable Presentation)를 의사에게 제출해 원격진료를 받는다. 이때 환자가 제출한 VP에는 환자의 이름과 주민등록번호들이 포함되어 있다. (2) 의사는 진찰하고, 환자에게 처방전 및 환자가 제출한 속성들을 포함하여, 환자에게 VC(Verifiable Credential)를 발급한다. (이 VC는 편의상 A VC라 부른다). (3) 환자는 약국에 A VC에서 조제를 위해 필요한 정보들을 택해 A VP를 만들어 A VC의 DID와 함께 제출한다. (4) 약국은 환자가 제출한 DID를 블록체인 원장에서 확인하여 처방전이 의사가 처방한 것이 맞는, 조작되지 않은 처방전임을 확인한다. 그 뒤 환자가 제출한 VP를 택하여



[그림 1] DID를 활용한 의약품 운송시스템

환자의 공개키로 암호화하여 QR코드 형식으로 박스에 기재한다. (환자가 제출한 VP를 환자의 공개키로 암호화한 것을 편의상 C라 부른다). (5) 물류는 배송인에게 전달되고, (6) 배송인은 앱을 통해 택배의 QR코드를 스캔해 택배함/잠금장치에 C와 DID, 공개키를 전달한다. (7) 배송인은 물류를 택배함/잠금장치에 전달한다. 수취 과정에서 환자는 (8) 앱을 통해 DID를 제출해 택배함/잠금장치에 저장된 C를 수신하게 된다. (9) 환자는 전송받은 C를 개인키로 복호화해 평문을 확인한 뒤, 해당하는 속성(VP)을 제출한다. (10) 택배함/잠금장치는 전송받은 속성(VP)을 보유하고 있는 공개키로 암호화해 C'를 생성한다. (11) 암호화한 C'와 이미 가지고 있는 C가 일치하면 잠금장치를 해제한다.

3.2 보안성 분석

3.2.1 물리적 문제

의약품 배달앱 시스템은 비대면 방법이 아니며, 현재 등기로 운용되고 있는 방법도 결국 대면을 통한 방법이다. 2021년에 서비스한 닥터나우의 조제약 배달 서비스는 비대면 방식이지만 문손잡이나 우편함에 운송하고 있다. 이는 제삼자가 의약품을 탈취하기 쉬우며, 민감한 의약품에 대해 원격 시스템이 자리 잡는 데 문제로 발생할 것이다. 이에 DID 잠금장치가 있는 곳에 운송하면 물리적 탈취를 예방하면서, 본인이 수령하게 되는 완전한 비대면 시스템으로 거듭날 수 있을 것이다.

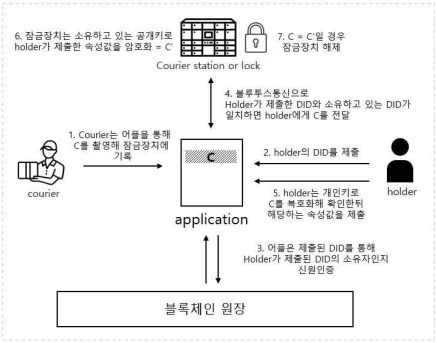
또한 단순한 운송시스템은 오배송으로 인해 신체에 물리적으로 손상을 입을 수 있지만, 해당 DID를 이용해 잠금장치를 개폐하게 되면 반드시 본인에 해당하는 DID를 제출하기 때문에 오배송의 위험이 사라질 것이다.

3.2.2 사이버공격

단순히 물리적 탈취를 막기 위해 잠금장치를 사용한다고 해도 제삼자의 탈취나 사이버공격으로 인한 개폐에서 자유로운 것은 아니며, 처방전의 진위를 확신할 수 없다. 그러나 일반적인 앱이 아닌 블록체인을 사용한다면 의사가 환자에게 VC를 발급할 때 블록체인 원장에 기록이 있어 약국에서 해당 처방전의 진위 판별을 할 수 있다.

또한 [그림1]의 (4)와 (9)~(11)의 과정에서 환자가 제출한 VP를 암호화하게 되면 일반적인 터치패드 형식의 고정 비밀번호가 아닌 매번 바뀌는 암호시스템이므로 비밀번호를 재사용하지 않게 되며, 여러 번의 인증과정을 거치게 되기 때문에 보안에 효과적이며, 암호를 주기적으로 바꾸지 않는 이유인 편의성에서도 뛰어난 효과를 보일 것이다.

해당 방식과 비교하여 환자는 VC DID를 전달하고, 택배함이나 잠금장치가 블록체인 서버와 통신을 통해 인증하는 방식도 안전한 방식이지만 [4] 해당 방식에 있어서는 디도스를 막기 어렵지만 [그림 2]와 같이 택배함 및 잠금장치가 암호화된 C를 보유하고 있고, 이를 복호화하여 해당하는 평문을 제출하는 방식을 사용하면 인증하는 과정에서 (3)을 유동적 인증 방식으로 남겨두면, 서버와 통신이 안되는 상황에서도 보안성이 있는 본인인증을 통해 잠금장치를 개폐할 수 있다.



[그림 2] DID 신원인증 과정 및 잠금장치 해제 과정

[그림 2]와 같이 환자가 제출한 DID를 통해서 네트워크가 되는 상황에서는 블록체인 원장을 통한 신원인증 방식으로, 단순한 공개키 전달로 잠금장치를 해제하는 방식에 비해 보안성을 더 강화하였다.

Ⅳ. 결론

정보통신 기술이 발전하고, 코로나로 인해 원격에 대한 수많은 정책이 시행되고 있지만, 편의성이 아닌 보안성 검토가 더 이루어져야 한다. 이에 의료 분야에 블록체인 기술을 도입하면서 처방전의 무결성이나 신원인증을 통해, 민감한 의약품에 대해서도 산업이 발전하게 될 수 있도록 하고자 한다. 제안한 의약품 운송시스템을 통해 물리적 탈취와 DID 사용으로 보안성을 높이는 동시에, 사이버공격을 막고자 하였다. 블록체인을 이용한 해당 시스템이 잠금장치에 사용되어 의료 분야를 넘어서, 여러 분야에서 개인의 자산을 지킬 수 있게 되기를 기대한다.

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] 최연석, “원격의료의 도입에 관한 연구 - 코로나바이러스감염증19 전염병과 원격의료 도입의 필요성 -”, 05. 2020.

[2] W3C, Decentralized Identifiers (DIDs) v1.0

[3] 홍상태, “원격진료 처방에 의한 의약품 배달앱 시스템 운영체계 개발”, 02. 2021.

[4] 전삼구, “블록체인을 이용한 물품 배송 박스의 보안 시스템 및 그 방법”, 04. 2021.

[5] Sarah Pearman, “Why people (don’t) use password managers effectively”, August. 2019.