Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.6, Dec. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.6.1103

OAuth 2.0 위임 Token을 이용한 환자정보 전달 시스템*

박 정 수,[1†] 정 수 환[2‡]
[1,2]숭실대학교 (대학원생, 교수)

Patient Information Transfer System Using OAuth 2.0 Delegation Token*

Jungsoo Park,[1†] Souhwan Jung[2‡]
[1,2]Soongsil University (Graduate student, Professor)

요 약

병원에서는 의료 기록저장 시스템 EMR (Electronic Medical Record)을 통하여 개인 정보 및 건강 정보를 저장 및 관리한다. 그러나 병원의 정보 공유를 위한 다양한 서비스를 제공함에 따라 취약점과 위협이 증가하고 있다. 따라서 본 논문에서는 EMR에서 환자 정보의 전송으로 인한 개인 정보 유출을 방지하기 위한 모델을 제안하였다. 환자의 의료 기록이 저장된 병원으로부터 환자 정보를 안전하게 수신 및 전달할 수 있는 권한을 부여하기 위한 방법을 OAuth 권한 위임 토큰을 사용하여 제안하였다. OAuth Token에 의사 정보와 환자가 원하는 기록 열람 제한을 적용하여 전달함으로써, 안전한 정보 전달이 가능하도록 프로토콜을 제안하였다. OAuth Delegation Token은 환자 정보를 열람할 수 있는 권한, 범위, 파기 시점 등을 작성하여 전달 가능하다. 이를 통하여 안전한 환자 정보 전달 및 환자 정보 재사용 금지를 방어할 수 있다. 또한, 불법적인 환자 정보 수집을 방지하고 전달 과정에서 발생할 수 있는 개인 정보의 유출을 방지한다.

ABSTRACT

Hospitals store and manage personal and health information through the electronic medical record (EMR). However, vulnerabilities and threats are increasing with the provision of various services for information sharing in hospitals. Therefore, in this paper, we propose a model to prevent personal information leakage due to the transmission of patient information in EMR. A method for granting permission to securely receive and transmit patient information from hospitals where patient medical records are stored is proposed using OAuth authorization tokens. A protocol was proposed to enable secure information delivery by applying and delivering the record access restrictions desired by the patient to the OAuth Token. OAuth Delegation Token can be delivered by writing the authority, scope, and time of destruction to view patient information.This prevents the illegal collection of patient information and prevents the leakage of personal information that may occur during the delivery process.

Keywords: OAuth, EMR, Delegation Token, JWT

Received(06. 16. 2020), Modified(10. 20. 2020), Accepted(10. 21. 2020)

* 이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행하였습니다. (No.2019-0-00477, 가상화된 신뢰실행환경을 이용한 안드로이드 보안 프레임워크 기술 개발) 또한, 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업의 연구결과로 수행하였습니다. (IITP-2020-2020-0-01602)

† 주저자, ddukki86@bufs.ac.kr
‡ 교신저자, souhwanj@ssu.ac.kr(Corresponding author)

I. 서 론

어러블의 발전과 함께 건강 정보를 지속적으로 병원에 저장하여 다양한 병원이 활용하기 위한 병원 통합 진료 시스템을 구축하여 정보를 전달하는 것이 국가적으로 큰 이슈로 떠오르고 있다. 하지만 병원마다 각기 다른 의료 플랫폼에 의하여 현재까지는 제대로 이루어지지 않고 있었다[1]. 한국에서는 2018년 전국 병원이 진료정보를 교류하는 통합 시스템을 구축하기 위하여 정부 부처 간 협업을 통하여 진행하였다[2]. 정보 중계를 위한 메타데이터 통합 저장소를 만들고 이를 국제 진료정보 교류 표준인 IHE 프로파일과 HL7을 적용하고, 진료의뢰와 회신서 작성 기능을 EMR 시스템과 연계하여 진료 정보를 제공하게 된다. 이를 통하여 기초정보를 한곳에 모아 병원이 원하는 정보를 빠르고 효율적으로 공유하기 위함이다. 하지만 국제 표준인 HL7은 아직 보안 프로토콜이 완벽하지 않아 위, 변조의 가능성이 크며 클라우드에 올라가는 중앙 집중식으로 될 경우 메타데이터에 대한 보안 위협에 대하여도 문제가 제기되면서 개인정보보호에 대한 이슈가 발생하고 있다[3][4]. 또한, 이러한 중앙 집중형 환자 정보 공유 시스템의 경우, 악의적인 병원에서 환자 기록을 지속적으로 수집하고 판매하는 등의 행위가 발생하여 안전하게 환자 정보를 보호하는 것이 큰 이슈가 되고 있다[5]. 따라서 본 논문에서는 OAuth 2.0 위임 토큰을 통하여 안전하게 정보를 전달받는 프로토콜을 설계하고 안전성을 분석하였다. 기존의 병원 통합 진료 시스템의 경우 통합 서버에 환자 정보가 등록되어, 의료진으로 인증 될 경우 환자 정보를 쉽게 획득할 수 있어 개인 정보 유출에 대한 문제점이 제기되었으나, 본 논문에서는 OAuth의 Token delegation 기능을 이용하여 일회성으로 환자 정보를 획득하는 방법을 이용하기 때문에, 환자 정보를 안전하게 전달하고 수집이 불가능하도록 설계하였다.

본 논문은 2장에서 국내외 의료정보 전달 현황을 분석하고 3장에서 환자정보 전달 시스템의 문제점 및 요구사항을 분석 한 후, 4장에서 기존 Delegation 모델에 대하여 분석하고, 5장에서는 안전한 환자정보 전달을 위한 모델을 제안하며, 6장에서 보안 고려사항에 대하여 분석한 후, 7장에서 결론을 내린다.

II. 국내외 환자 정보 전달 시스템

2.1 국내

전자의무기록에는 개인의 병력, 현재의 투약상태, 검사결과 등의 건강정보를 쉽게 입력하고, 저장하며, 사용자들이 이용하기 편리한 형태로 처리하여 제공되고, 사용자간에 정보 교환을 용이하게 하며, 정보 안정성을 모두 제공할 수 있어야 한다[6]. EMR 을 비롯한 다양한 헬스케어 서비스 구조는 보안상 취약성과 공격에 노출 될 위험이 크다. 특히, 네트 워크에서 발생 및 교환되는 정보는 극히 개인적인 건강정보, 생활 습성, 신체적 특징 등과 같이 프라이버시에 민감한 정보들이 대부분이고 거주자의 건강과 생명에 연관성이 있는 민감한 정보들이 대 부분으로서 서비스에서의 정보보호는 안전하고 신뢰성을 보장하기 위한 방안이 필수적으로 고려되어야 한다[7][8]. 국내에서는 전자의무기록(EMR)과 관련된 환자 정보보호에 관하여 의료법 및 보건의료법제를 포함하고 있다. 전자의무기록은 한 개인의 건강 상태가 의학적 문제가 전자 형태로 저장되어 사용되고 있으나 아직 전 세계적으로 통일되어 사용되고 있지는 않다. 하지만 보건의료정보의 공유 또는 공동 활용으로 인하여 개인 정보 침해 발생이 될 수 있다는 점이 지속적으로 문제제기가 되고 있다. 특히, 최근 정보통신망을 이용한 의료정보 공유를 추진하고 있어 법 제정 및 연구를 지속적으로 수행하고 있는 추세이다.

2.2 국외

미국의 경우 연방특별법 제정 전 개인정보에 관련된 법률에 기초하여 보건의료 정보를 보호하였고, 보건의료기록은 일찍부터 주법에서 상호 상이한 수준에서 보호하고 있는데, 정보화가 가속화됨에 따라 주사이에 보건의료정보의 이전과 그 표준화가 문제되었다. 따라서 보건의료정보에 대한 통일법이 논의 되었고, 그 시도가 '통일보건 의료정보법(Unifrom Healthcare Information Act; UHIA)'의 제정으로 나타났다. 미국의 의무기록연구소는 전자의무기록(EMR)의 발전단계를 5단계로 구분하여 설명하고 있다. 1단계는 의무기록 자동화로 보험 및 청구의 자동화를 위한 전산화, 환자 관리를 위한 등록을 자동화 하는 단계이다. 2단계는 의무기록의 전자보관 단계로 의무기록을 사진으로 찍어 컴퓨터에 저장하는

단계를 의미한다. 3단계는 전자의무기록으로 의사의 처방이 내려지면 고쳐지지 않는 하부 구조를 가지고 기록하는 단계이다. 4단계는 전자의무기록 시스템으로 EMR 체계가 국가 적인 표준을 설정하여 상호 호환성이 있어야 함을 의미한다. 5단계는 전자건강기록으로 환자 의료정보, 민간의료에 대한 모든 사항을 포함하고 있다[9].

일본에서는 전자카르텔 이라는 명칭의 EMR을 도입하여 일본 보건의료복지정보시스템공헙회에서 제정하여 사용하고 있다. 1단계는 의료기관 내 개별 전자 공유 단계이며, 2단계는 의료 기간 내 복수의 전자 공유 단계 3단계는 개별 환자 정보 공유화 단계, 4단계는 복수의 기관과 상호 공유 단계, 5단계는 의료정보뿐 아니라 사후 관리 과정을 포함한다. 특히 일본은 현재 EMR 보급률이 40%에 불과하여 환자의 편의성을 위해 병원간 정보공유 네트워크가 필요하다는 것을 인지하고 도쿄 의사회에서 환자 정보 공유를 위하여 기관당 약 16만달러가 필요하다고 제안하자 병상 20개 이상의 의료기관이 참여할 경우 한 곳당 8만엔을 지원하는 등의 지원을 하고 있다[10].

III. 환자 정보 전달 시스템 관련 연구

3.1 환자 정보 전달 시스템의 문제

2016년 5월 구글 인공지능 자회사 딥마인드와 영국 의료보험기구(National Health Service: NHS)가 맺은 데이터 공유 협약이 문제가 되었다. 런던 병원의 160만 환자에 대한 데이터가 구글 인공지능 자회사인 딥마인드에 전달되었기 때문이다. 구글에서는 연구목적인 데다 익명처리된 데이터라고는 하지만, 민감한 의료 검사 데이터들이 다수 포함돼 있어 개인의료 정보 보호에 대한 우려의 목소리도 높아지고 있다. 이렇게 의료법에 명시되어 있지 않은 개인정보에 대한 공유가 발생하는 경우가 있어 전 세계적으로 문제가 제기되고 있다[11].

한국에서는 개인정보보호법에 의거하여 진료기록부, 수술기록부, 조산기록부, 간호기록부, 환자명부 등 진료를 목적으로 수집하여 처리하는 개인정보가 포함된 정보가 개인정보보호법에 적용되나, 개인정보보호법보다 의료법을 우선 적용하고 규정이 없는 경우 개인정보보호법을 적용하는 것을 원칙으로 하고 있다. 의료법 제22 조(시행규칙 제14조)에 따르면 개인 정보에 대한 수집의 건이 환자 동의 없이 수집은 가능하지만 진료목적으로만 사용이 가능하다는 것으로 표현하고 있다[12]. 이와 같이 환자 동의 없이 수집이 가능하기 때문에 다양한 악용 사례가 발생할 수 있으며 기존 연구에서 진행된 환자 전달 정보 시스템에서는 아래와 같은 추가적인 문제가 발생할 수 있다. 중앙 집중 시스템에 존재하는 환자 정보를 열람할 수 있는 권한이 병원 스태프에게 존재한다. 환자 정보에 대한 열람을 병원 스태프가 하게 될 경우, 병원 스태프는 타 병원 환자에 대한 열람을 통하여 정보를 획득할 수 있다. 이는 개인정보 유출의 문제를 가지고 있으며, 악의적인 병원 스태프가 다수의 환자 정보를 수집하여 판매 목적으로 악용할 수 있다는 점이다.

병원간 환자 정보 전달의 경우, 응급 환자가 입원한 병원에서 기존 환자 정보를 보유한 병원에 요청하게 되는데, 이런 경우 환자의 동의 없이 환자 정보를 열람하여 전달한다는 점에서 문제가 발생할 수 있다. 기존 병원에서는 환자가 응급으로 입원하였는지 확인할 수 없다는 단점을 가질 수 있기 때문이다.

중앙 집중 시스템에 존재하는 환자 정보는 네트워크 접근, 웹 서버 관리, 보안 시스템에 의한 관리 등의 부재로 인하여 공격 받을 경우, 다수의 환자 정보가 유출될 수 있다는 점에서 문제가 발생할 수 있다. 특히 환자 개인의 정보가 암호화 되어 저장되어 있더라도 중앙 집중 시스템에 모든 정보가 모여 있는 것은 SPOF의 문제를 발생시킬 수 있으며 바이러스, APT 공격 등에 의하여 공격자의 타겟이 될 수 있다.

또한, Chong Min Hon et al. 등은[13] 처방전달시스템의 보안 취약점을 분류하였는데, 비인가자의 시스템 접근, 의료정보 취급 보안 서약 부재, 의료정보 취급자 권한 관리 부실, 비인가자의 데이터베이스 접근, 의료정보 및 개인정보 관리 부실, 의료정보 출력본 관리 부실 등을 꼽고 있다. 특히, 보안 서약 부재로 의료정보 분쟁 시 책임소재에 대한 내용과 직원 고용조건 변경 및 퇴사 후 의료정보 분쟁 시 책임 소재, 의료정보 가치, 업무, 영향, 법적 준수사항이 고려되지 않은 상태에서의 의료정보 무차별 수집, 내부 의료정보 취급자 및 퇴사자에 의한 의료정보 유출은 심각한 문제로 제기하고 있다.

Table 1. Threats to patient information delivery systems[13]

Category	Threat
Unauthorized access and server attacks	- It is possible to obtain patient information through the distribution of malicious codes. - Server and database attack by APT is possible. - Illegal inquiry, tampering, and leakage through authentication bypass and illegal user creation are possible.
No security pledge for handling medical information	- Due to lack of security pledges, the responsibility for medical information disputes is unclear. - Responsibility for medical information disputes after changing employment conditions and leaving the company is unclear.
Poor management of medical information handler rights	- Indiscriminate collection of medical information may be performed without considering the medical information value, business impact, and legal compliance matters. - It is possible to leak medical information by internal medical information handlers and retirees.
Poor management of printed medical information	- It is possible to leak copies and copies of personal and medical information. - Due to the absence of a media copy approval process, it may be unclear where the material is responsible for spills.

3.2 환자정보전달 시스템 요구사항

환자의 정보처리에 있어, 안전한 클라이언트/서버 기반의 시스템 환경이 구축되어야 한다. 환자정보전달 시스템 전체에 접근 통제가 이루어져야 할 뿐 아니라, 의료정보 취급자에 대한 접근 통제 및 모니터링은 필수적인 요소이다. 네트워크 보안, 운영체제 보안, 접근제어, 악성코드 탐지 등에 대한 솔루션들이 적용되어야 하며 의료 정보 취급자에 대한 보안, 의료정보 취급자 등록 및 관리, 권한 관리, 패스워드 관리 등도 이루어져야 할 것이다. 특히 한국에서는 의료법 제 22조, 23조에 의거 의료정보에 관련한 데이터 접근 통제 및 자산에 대한 정보 조사 법률이 제정되어 있다. 자산별 가치, 업무 영향, 법적 준수사항이 고려되어 중요도가 정해진 의료정보 및 관리 체계 및 암호화 강도 및 수준이 적용되어야 한다. 또한, 데이터베이스 관리자 및 사용자 식별, 접근통제, 암호화 키 관리 등이 같이 이루어져야 한다. 제공되는 환자 정보에 대하여 개인정보 마스킹을 통하여 개인정보 표시가 제한되어야 하며, 개인정보의 취급 및 보관, 폐기 시점 또한 결정되어야 한다[14].

IV. 관련 연구

4.1 Delegation을 통한 정보전달 시스템

웨어러블 디바이스와 같은 센서 환경과 함께 유, 무선 네트워크와의 융합기술을 활용하여 간단한 진료부터 원격진료, 맞춤형 의료기술 등 언제 어디서나 진료 및 치료를 받을 수 있게 하는 서비스인 스마트 의료는 지속적으로 연구되고 발전하고 있다. 특히, IoT 환경에서 환자 정보를 공유하거나 권한을 위임하는 연구에 대한 논문은 다양하게 진행되어 왔다. 대부분 서버기반의 Delegation 모델을 제시하고 있으며, 본 논문에서는 4가지의 Delegation 모델을 분석하고 추후에 제안하는 프로토콜과 비교 분석하고자 한다.

첫 번째로, Dasun Weerasinghe et. al 등은 [15] 환자 기록은 의료 센터에 저장되어 있고, 응급상황에 있는 경우 모바일 기기로는 환자 정보를 획득할 수 없기 때문에, 환자 정보를 획득하기 위하여 신뢰할 수 있는 서버를 이용하여 health staff가 인증하고 환자 정보를 가져오게 되는 형태의 모델을 제안하였다. Staff의 level을 1부터 10까지 나누어 10

은 높은 신뢰 수준, 1은 낮은 신뢰 수준으로 의료 스탭의 레벨을 나누어 접근 권한을 부여하였고, Token 암호화를 위하여, key 생성은 IMPI(모바일 장치의 SIM 카드 번호), IMEI(모바일 장치 고유번호), Authentication ID를 이용하여 암호화 하였다. 또한, Token 파기를 위하여 TGS(Ticket Granting Service) 타임스탬프 값과 Token 생성 타임스탬프 값을 전달하게 되고, 일정 시간 후 파기할 수 있도록 하였다. 이러한 방법은 TGS를 통하여 병원 스태프들이 인증을 받고, 이를 이용하여 환자의 정보를 전달해주기 때문에 Delegation의 역할이 충분히 수행되며, TGS를 Trust한다고 간주하기 때문에 안전한 정보전달이 된다고 주장하고 있다. 하지만 이러한 시스템은 악의적인 병원 스태프로 인한 환자 정보 획득 및 수집이 가능하며 이를 통한 개인정보 유출이 가능한 문제점을 지닌다. 또한, 요청된 환자의 정보가 실제로 병원에 응급환자가 있는 사실을 확인 할 수 있는 방법을 정의 및 해결하지 못하고 있다. 더 나아가, 모바일 환경을 고려하여 IMPI, IMEI, AU-ID를 이용하여 인증을 수행하였으나 IMPI/IMEI 값 등은 개인정보로 취급될 수 있어 인증 아키텍처의 위험요소가 될 수 있다.

두 번째로, ByungKwan Lee et. al 등은[16] 클라우드 기반에서 환자 정보를 전달하는 방법을 제안하였다. 인증기관으로부터 인증 받은 사용자만이 클라우드 서버에 저장된 데이터에 접근할 수 있도록 제어하고, 역할속성과 상속유효시간을 Permission에 추가하여 위임을 받은 사용자들만이 데이터에 접근하도록 제어하였다. 하지만 정보 전달 시간을 클라우드에 정해놓은 시간으로 한다는 점에서 일회성이 떨어져 지속적인 다운로드가 가능하다는 단점이 있다.

세 번째로, Bum-ki Lee et al. 등은[17] Capability based Access Contorl 모델을 제시하였다. ACL(Access Control List)을 만들어 사용자가 자원에 대한 연산을 요청할 경우에 서비스 제공자는 사용자가 직접 또는 간접적으로 객체에 대한 권한이 있는지의 여부를 확인한 후, 요청한 자원 또는 요청한 연산을 수행할 수 있도록 인가하는 모델을 제시하였다. Capability는 주체가 새로운 객체를 생성할 수 있고, 또한 그 객체에게 허용되는 권한을 정의하는 것으로, CL(Capability List) 기반 접근 제어는 주체에게 부여된 권한을 통해 주체가 객체에 접근하며 이러한 권한은 다른 주체에 위임이 가능하다. 사용자는 자신의 capability와 함께 자원에 대한 접근 요청을 보내게 되고, 자원에서 capability의 검증을 통해 자원에 대한 액세스 여부를 결정하게 된다. 이것은 기존의 Access Token 대신 Capability Token을 사용하여 ACL과 달리 사용자가 자신의 Capability를 가지고 접근하는 방식을 제안한 것으로 위임은 자원 제공자로부터 진행되나, Token이 이미 발행된 경우 유효성만 검사하기 때문에 토큰이 노출될 경우, 이 토큰이 언제 어떻게 누구에게 쓰이는지 확인할 수 있는 방법이 없다는 점에서 단점이 있다.

각각의 모델들은 서버에 사용자 별 권한을 저장하고 이를 통한 관리 및 위임을 진행하는 방식이다. 하지만 이러한 방식을 병원 시스템에 접목시킬 경우, 악의적 병원 staff 혹은 병원 시스템 자체에서 지속적으로 환자 정보를 수집할 수 있는 문제를 가지고 있을 뿐 아니라, 중간 서버가 환자 정보를 확인할 수 있다는 점에서 개인 정보 보호에 취약하다. 또한, SPOF(Single Point Of Failure)와 같이 중앙 서버의 고장으로 인하여 환자 medical 및 healthcare 정보가 전부 삭제되어 불편함을 초래할 수 있다. 따라서 이러한 문제를 해결하고자 중앙 서버 기반이 아니고, 각 병원에서 서버를 보유하고 신뢰할 수 있는 권한 위임자를 통한 환자 정보 전달에 대한 연구를 진행하였다.

4.2 OAuth 2.0 및 Token Delegation

OAuth 2.0은 네 가지 grant type을 이용하여 상황에 맞게 사용이 가능하다[18][19]. 각 grant 방식은 다음과 같다. Authorization code 방식은 가장 많이 사용되는 방식으로 장기 접근이 요구될 때 사용하며 이때 OAuth 클라이언트가 웹 애플리케이션 서버여야 하고, API 호출에 대한 책임이 매우 중요하고 사용자가 접근하는 웹 브라우저에 OAuth 토큰이 노출되지 않아야 할 때 사용하는 방식이다. Implicit 방식은 데이터에 접근이 일시적으로 필요할 때 사용하는 방식으로 사용자가 규칙적으로 API 제공 업체에 로그인하거나, 웹 브라우저의 신뢰도가 높고, 신뢰할 수 없는 사용자나 애플리케이션에 노출될 염려가 적을 때 사용한다. 하지만 재발급을 할 경우 위험에 노출 될 수 있어, refresh token은 발급하지 않는다. 또한, 권한 서버가 규칙적으로 액세스 토큰을 만료하면, 애플리케이션은 접근이 필요할 경우 권한 플로우를 다시 진행해야 한다. Resource

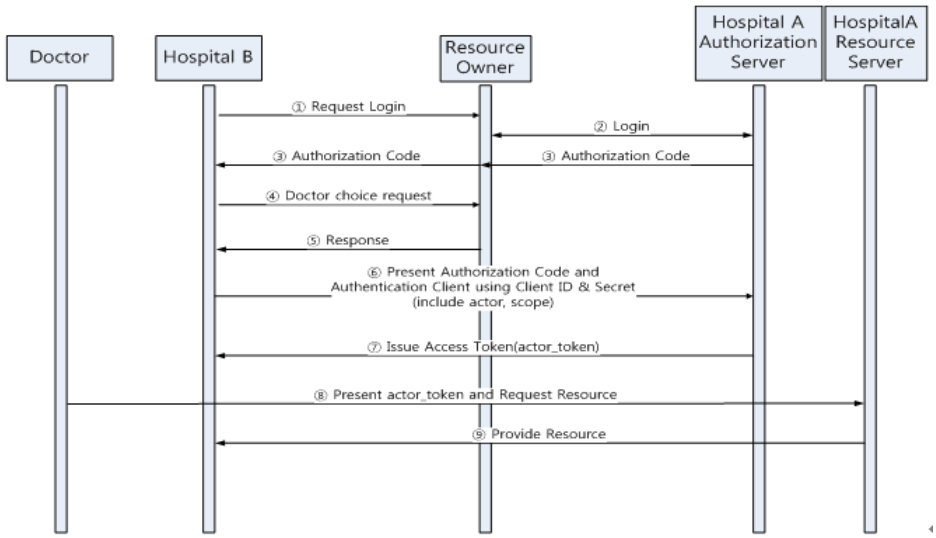


Fig. 1. Proposed Model Flow

Owner password credentials 인증 방식은 Resource owner와 client 사이의 관계가 믿을 만한 경우에 사용하고 보통 API 제공 업체가 배포한 공식 어플리케이션에 사용한다. 마지막으로 Client Credentials 인증 방식은 Client가 resource에 대한 접근 권한을 가지는 방식으로client가 데이터를 소유하고 있어서 resource owner에게 접근을 위임 받을 필요가 없거나, OAuth 플로우 외부에서 애플리케이션에 접근 위임이 이미 허용되었을 경우에 사용하는 방식이다[20].

V. 제안모델

5.1 제안모델 설명

이번 섹션에서는 OAuth Token Delegation 모델을 이용하여, 안전한 환자 정보를 전달하는 과정을 설명한다. 모든 과정은 SSL 채널이 형성되어 있어야 동작 가능하다.

1. 병원 B는 OAuth를 통해 환자에게 인증 페이지를 요청한다.
$$Request(OAuth\,Page) \quad (1)$$
2. 통합 시스템에서 환자는 A 병원에서 사용되는 자신의 ID로 로그인한다.
$$User\,Login(using\ id/pw, H_A) \quad (2)$$
3. 병원 A는 환자의 로그인 정보를 확인하고 Autorization Code를 전달한다. 이과정에서 client id는 서비스 API 컨슈머 키로, OAuth 인증을 위해 발급받은 ID 이다. Redirect URI의 경우, Authorization Code 발급 후 전달할 URL로서 인코딩되어 있다. State는 CSRF (Cross-site request forgery)를 방지 하기 위한 정보이다. Domain은 실제 사용되는 도메인 명을 의미한다.
$$JWT = client\,id, redirect\,uri, state, domain \quad (3)$$
4. 병원 B는 환자가 의사를 선택할 수 있는 페이지를 제공하며, 이것은 나중에 발행 될 의사 정보를 토큰에 “act” 영역에 적용한다.
5. 환자는 의사를 선택하면서 의료 기록의 어느 부분에 액세스 할 수 있는지 선택하게 되며, 토큰의 “scope”영역에 적용된다.
6. 병원은 승인 된 의사(act) 및 승인 된 범위(scope) 값으로 Autorization Code를 보낸다. 이때 JWT는 {header BASE64 인코딩}.{JSON Claim set BASE64 인코딩}.{signature BASE64 인코딩}의 형태로 전송되게 된다. 수식 (4)에는 JWT Header 영역에 실제 저장될 때, RSA SHA-256으로 암호화하여 전송하는 것을 명시하여 보내야 한다.

Table 2. JWT Notation[21]

Name	Definition
Iss	Identifier (e token. Typically a DNS name, but doesn't or, name) of the server or system issuing th have to be.
Iat	Date/time when the token was issued.
exp	The validity lifetime, in seconds, of the token issued by the authorization server.
aud	The logical name of the target service where the client intends to use the requested security token.
sub	Identifier (or, name) of the user this token represents.
act	JWT to express that delegation has occurred and identify the acting party to whom authority has been delegated.
scope	if the scope of the issued security token is identical to the scope requested by the client

$$JWT\ Header = 'alg' : RS256, 'typ' : JWT \quad (4)$$

7. 병원 A는 행위자와 범위를 포함하는 액세스 토큰을 발행한다. 토큰의 기본 구조는 OAuth 2.0 표준[21]을 참조하였다. 예제 표에서 exp 및 nbf와 같은 시간 정보는 NumericDate 값을 사용한다. 범위의 경우 약어는 각 의료 용어에 대해 표시된다. 또한, Token의 scope를 이용하여 저장, 출력 및 인쇄와 같은 정보를 제한하도록 범위를 조정할 수 있다. 그림 2와 그림 3는 jwt에 정보를 입력하기 위한 화면이며, 그림 4는 입력 값을 기반으로 클레임 집합이 있는 화면이다. 마지막으로, 그림 5는 생성 된 jwt 토큰이 올바르게 디코딩되었는지 확인하는 화면입니다.
8. 의사는 통합 시스템에 액세스 할 수 있는 경우 토큰을 통해 정보를 요청한다.
9. 마지막으로 환자 정보를 받아오게 된다.

이 시스템은 이전 서버 기반 환경과 비교하여 더

Fig. 2. Standard JWT Claims

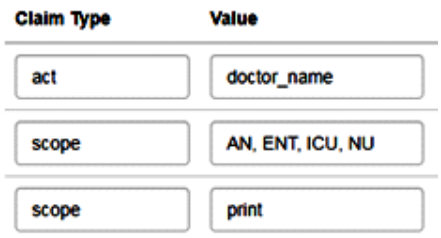


Fig. 3. Additional Claims

```
{
    "iss": "https://Hostpital A.com",
    "iat": 1582249083,
    "exp": 1613785083,
    "aud": "https://Hostpital B.com",
    "sub": "patient@email.com",
    "act": "doctor_name",
    "scope": [
        "AN, ENT, ICU, NU",
        "print"
    ]
}
```

Fig. 4. Generated Claim Set (plain text)

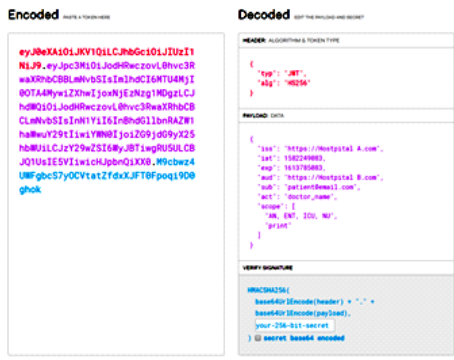


Fig. 5. Decoded JWT Token using JWT Decoder

Table 3. Comparison with existing scheme

	Proposed model	[15]	[16]	[17]
Information storage location	Individual storage of data	Centralized	Centralized	Individual storage of data
Information access	OAuth token based	Only authorized users access	Only authorized users access	OAuth token based
Information disclosure scope	The patient's own decision	Centrally managed by applying capability	Centrally managed by applying permission	Centrally managed by applying capability
Information reuse	Not reusable	possible	possible	possible
Whether or not information is saved	The patient's own decision	Information delivery and automatic storage	Information delivery and automatic storage	Information delivery and automatic storage

복잡한 흐름을 가질 수 있지만 강점은 직원이나 병원이 환자의 동의 없이 정보를 수집 할 수 없고 환자의 민감한 개인 정보가 유출 될 위험을 줄일 수 있다. 또한, 중앙 집중형 서버 방식에서는 해커가 하나의 서버를 공격하여 환자 정보를 모두 획득할 수 있는 취약점이 있지만, 제안하는 모델은 환자 정보를 얻기 위해 각 병원의 서버를 공격해야하기 때문에 중앙 집중형 서버 방식에 비해 안전합니다. 다음 섹션에서는 보안 고려 사항을 추가로 분석한다.

VI. 제안 모델 보안성 분석

6.1 정보 저장 및 전송

이 연구에서 환자의 의료 및 건강 정보는 각각의 병원에 저장된다. 이 정보는 병원의 독립 서버에 저장되고 OAuth 모델을 기반으로 열람 및 다운로드 등의 권한을 받아 수행하게 된다. 기존과 달리, 의료진이 쉽게 열람할 수 있는 것이 아니라 환자가 의사와 의료 정보 수집에 대한 범위를 제공하기 때문에 의료진은 지속적으로 환자 정보를 수집할 수 없다. 또한, OAuth 토큰 기반으로 권한 인가자에 대한 검증이 바로 이루어 질 수 있어, 누가 언제 어떤 곳에서 다운로드가 이루어졌는지 확인이 쉽게 가능하다. OAuth로 인증을 수행한 경우, 본인의 자원서버로부터 직접 자원을 받아오는 과정을 수행하기 때문에 외부인이 자원 접근으로 인한 유출 위협도 발생하지 않는다. 또한, expire time외에도, OAuth의 경우, Token revocation time을 서버에서 설정할 수 있다. Token Revocation time이 1회로 지정되어 있는 경우, 한차례의 다운로드 이후, Token은 파기되고 다시 재사용이 불가하다기 때문에 악의적인 환자정보 수집을 막을 수 있다.

6.2 권한 위임 토큰 사용을 통한 안전한 프로토콜 활용

Token을 이용한 환자정보 위임을 위해 OAuth에서 제공 한 위임 토큰을 사용했다. 위임 토큰을 사용하는 경우 메시지는 HMAC SHA 256으로 인증되고 전송 된 base64로 인코딩된다. 서버에서 키를 도난당하지 않으면 이를 가로 채서 재사용 할 수 없습니다. 이것은 권한 위임을 통해 안전한 환자 정보 전달을 보장한다.

6.3 기존 연구와의 비교

기존 연구와의 비교를 위하여 환자 정보 저장 위치, 환자 정보 접근 위험성, 정보 접근성으로 분류하여 아래와 같이 비교하였다. 제안한 시스템의 경우, 기존 시스템에 비하여 정보 저장을 중앙 집중형에서 탈피할 수 있으며, 사용자 접근부터 인가된 사용자만 접근이 가능하며 정보 재사용이 불가능 하다는 점에서 장점을 가질 수 있다. 또한 데이터 자체를 웹 기반으로 열어보고 다운로드, 저장, 출력 등의 형식도 환자가 직접 선택할 수 있다는 점에서 장점을 가질 수 있다.

Table 4. Advantages through the proposed technique

Vulnerability	Defense technique
Unauthorized access and server attacks	Solve problems such as SPOF by constructing separate server for each hospital instead of centralized server
Medical information handler authority management mismanagement	It is possible to prevent the indiscriminate collection of medical information, so the existing problems can be solved
Medical information and personal information mismanagement	By limiting the scope of authority and the choice of authorized physicians, personal information can be prevented from leaking to the outside.

VII. 결 론

글로벌 IoT 건강 관리 시장은 2018 년까지 매년 10.2 % 성장 또는 121 억 달러로 추정되고 있다. 건강 관리 및 시장 개발에 대한 관심에 따라, 환자의 의료 기록을 공유하기 위해 연구 개발이 지속적으로 수행되고 있다. 국내 시장에서 병원들 사이에 건강 정보를 안전하게 전송하는 기술들이 제안되고 있다. EMR은 한국의 대부분의 병원에서 소개되어 적용되고 있으나, 한국의 경우 의료기관 간 정보 공유는 1.3 %로 제한되어 있으며 이는 환자 편의보다는 병원간 이해 관계로 제한되고 있다. 또한 불완전한 보안 프로토콜로 인해 다양한 문제가 제기되었으며, 문제를 해결하기 위해 다양한 연구가 추가로 필요한 실정이다.

이 연구는 의료 및 건강 정보가 병원의 독립 서버에 지속적으로 저장되고 관리되는 환경에서 환자가 병원 의사와 의사가 열람할 수 있는 범위를 제안하는 OAuth Token을 이용하여 환자 정보를 안전하게 전송하는 방법을 제안했다. 이 모델은 OAuth 프로토콜을 운영하기 위한 시스템이 적용되었다는 가정하에, 위임 된 병원 의사가 토큰을 사용하여 액세스 권한을 부여하는 방법을 사용하였다. 이를 통해 우리는 다른 병원에서 지속적으로 수집하거나 활용할 수없는 구조를 설계했으며, 환자의 요청이 있을 때만 병원간에 정보를 쉽게 전송할 수 있도록 하였다. 이 모델은 여러 환자의 정보 수집 및 환자 정보 유출과 관련된 문제를 해결할 수 있으며 중앙 집중형으로 인한 SPOF와 같은 문제도 해결할 수 있다. 이를 통하여 환자 기록의 안전한 공유와 관련된 최근의 문제를 극복 할 수 있으며 향후 실제 의료 산업에 적용될 수 있다.

References

[1] Esposito, Christian, Mario Ciampi, and Giuseppe De Pietro. "An event-based notification approach for the delivery of patient medical information." Information Systems 39 (2014): 22-44

[2] Chen, Hannah S., et al. "Blockchain in Healthcare: A Patient-Centered Model." Biomedical journal of scientific & technical research 20.3 (2019): 15017.

[3] Tobiano, Georgia, et al. "Patient engagement in admission and discharge medication communication: A systematic mixed studies review." International journal of nursing studies 95 (2019): 87-102.

[4] Oh, Am-Suk. "A Study on HL7 Standard Message for Healthcare System Based on ISO/IEEE 1107," International Journal of Smart Home 9.6 (2015): 113-118

[5] Tobiano, Georgia, et al. "Patient engagement in admission and discharge medication communication: A systematic mixed studies review." International journal of nursing studies 95 (2019): 87-102.

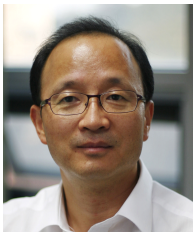
[6] Lee, Byung Mun, and Jinsong Ouyang. "Intelligent healthcare service by using collaborations between IoT personal health devices," blood pressure 10 (2014): 11

[7] Yea, Sang-Jun, Chang-Sop Yang, and

Chul Kim. "Design Korean Medicine Health Information Model 장
[8] with Health 2.0 Framework." The Journal of the Korea Contents Association 13.11 (2013): 807-814.
[9] Yun-Young Sok, and Seok-Hyun Kim "Integrated Medical Information System Implementation for the u-Healthcare Service Environment," The Journal of The Korea Contents Society14.5(2014):1-7.
[10] Goldstein, Melissa M. "Health information privacy and health information technology in the US correctional setting." American journal of public health 104.5 (2014): 803-809.
[11] Biller-Andorno, Nikola, and Thomas Zeltner. "Individual Responsibility and Community Solidarity—The Swiss Health Care System." New England Journal of Medicine 373.23 (2015): 2193-2197.
[12] Hawkes, Nigel. "NHS data sharing deal with Google prompts concern." BMJ 353 (2016): i2573.
[13] Kwak, Sang-Hyun, et al. "Current status of intensive care units registered as critical care subspecialty training hospitals in Korea." Journal of Korean medical science 29.3 (2014): 431-437.
[14] Chong Min Hong, and Weon Shin "Security Requirements of Order Communication System in Hospitals for Compliance with Personal Information Protection Act," Journal of Security Engineering Vol.10, No.5 (2013), 513-526
[15] Yoo, Sang-Ho, et al. "Ethical principles and practice guidelines concerning the usage of public database for medical researches." Journal of the Korean Medical Association 56.11 (2013): 1031-1038.
[16] Weerasinghe, Dasun, Yogachandran Rahulamathavan, and Muttukrishnan Rajarajan. "Secure trust delegation for sharing patient medical records in a mobile environment, Health Policy and Technology 2.1 (2013): 36-44.
[17] ByungKwan Lee, and EunHee Jeon "A Role based Health Data Access Control Model for Patient Information Protection on Cloud Computing Environment," Journal of Security Engineering Vol.13, No.3 (2016), 183-194
[18] Bum-Ki Lee, et al. "Design and Implementation of The Capability Token based Access Control System in the Internet of Things," Journal of The Korea Institute of Information Security and Cryptology 25.2 (2015): 439-448
[19] Campbell, B., et al. "OAuth Working Group Internet-Draft Intended status: Standards Track," 2012.
[20] Hardt, D., "The OAuth 2.0 Authorization Framework," RFC 6749, October 2012.
[21] Tassanaviboon, Anuchart, and Guang Gong. "Oauth and abe based authorizationin semi-trusted cloud computing: aauth," Proceedings of the second international workshop on Data intensive computing in the clouds. ACM, 2011.
[22] Jones, Michael, et al. "JSON Web Token (JWT)," RFCC 7519, may 2015.

〈저 자 소 개〉

박 정 수 (Jungsoo Park) 학생회원
2013년 2월: 숭실대학교 정보통신공학과 졸업
2015년 2월: 숭실대학교 전자공학과 석사
2015년 3월~현재: 숭실대학교 융합소프트웨어학과 박사과정
〈관심분야〉 모바일 보안, 클라우드 보안, 인증, 악성코드 분석



정 수 환 (Souhwan Jung) 종신회원
1985년 2월: 서울대학교 전자공학과 졸업
1987년 2월: 서울대학교 전자공학과 석사
1996년 6월: University of Washington 박사
1988년~1991년: 한국통신 전임 연구원
1997년~현재: 숭실대학교 전자정보공학부 교수
〈관심분야〉 클라우드 보안, 모바일 보안, 네트워크 보안