# PHR의 프라이버시를 보장한 키 분배 프로토콜

조영복* · 우성희** · 이상호*

*충북대학교 , 한국교통대학교

# A Key Distribution Protocols Ensure the Privacy for PHR

Young-bok Cho* · Sung-Hee Woo**

*Chungbuk National University

E-mail : bogicho@cbnu.ac.kr

## 요 약

개인의료정보(Persnal Healthcare Record:PHR)는 서버로 집합되어 관리되는데 문제점이 제시된다. 서버에 저장된 PHR은 매우 민감한 정보로 접근권한이 제한되어야 한다. 따라서 이 논문에서는 PHR의 접근권한을 구별하기 위한방법으로 각 접근자들의 역할을 기반으로 계층적 키를 분배함으로 PHR의 프라이버시를 보장하는 키 분배 프로토콜을 제안한다.

## ABSTRACT

PHR is integrated into the server, so the problem has managed. Thus, the highly sensitive information stored on the server. PHR should be limited to the access rights. In this paper, the access rights of PHR as a way to distinguish the role of each approach based on a distributed hierarchical key to ensuring the privacy of PHR by key distribution protocol is proposed.

## 키워드

u-Healthcare Service, PHR, EMR, Authentication, Privacy

## Ⅰ. 서 론

정보통신의 발전과 더불어 u-헬스케어 서비스의 급속한 발전과 이를 지원하는 다양한 서비스 기술의 많은 변화가 이루어지고 있다. u-헬스케어 서비스를 실현하기 위해 의료정보들은 디지털화 및 통합관리 되고 의료정보가 축적되면서 용이하게 열람 할 수 있도록 IT의 도입을 통해 전자의무기록 시스템의 도입 및 시행과 관련하여 현행 전자의무기록 시스템 활용시 개인의료정보(PHR : Persnal Healthcare Record))에 관한 보안 문제점들이 대두되고 있다[1,2,3,4].

또한 인터넷이나 무선통신 기기를 이용한 의료정보화를 통해 축적 및 교환되는 의료정보의 양이 폭발적으로 증가함에 따라 보호 대상 또한 급격히 증가될 것이다. 의료정보의 디지털화는 다양한 장점이 있지만 환자 개인의 프라이버시 침해 문제로 의도적인 유출이 생기거나 의료정보의 거래, 부정한 열람 및 복제의 위험성에 직면할 수 있다. 특히 어떤 종류의 의료정보는 고용차별, 사회적 차별 등으로 인한 정신적 고통이라는 큰 불이익을 낳을 수 있게 된다. 개인의료정보는 환자의 병력과 이름, 주소, 전화번호, 연령 등의 민감한 개인 정보들을 기록하고 있고 최근들어 DNA 의료 분석에 수반되는 유전정보들을 포함하고 있어 프라이버시 보호문제에 매우 민감한 데이터라고 할 수 있다. 그러나 의료진 또는 연구자에 의하여 부적절하게 이용될 경우, 개인의 프라이버시 침해로 이어질 수 있다.

이와 같이 개인의 프라이버시 정보인 의료정보는 안전하게 관리, 저장 및 유통되어야 한다. 의료기관 등에서 민감한 개인 의료정보를 데이터베이스에 보관하게 될 경우, 내부자 및 외부자로부터의 기밀성 유지가 필요하며, 또한 의료 서비스 내역 및 서비스 사용자에 대한 프라이버시 보호와 권한관리 유지가 필요하다. 따라서 디지털화된 의료정보의 프라이버시 보호를 위한 계층적 키분배 프로토콜이 필요하다[5,6,7].

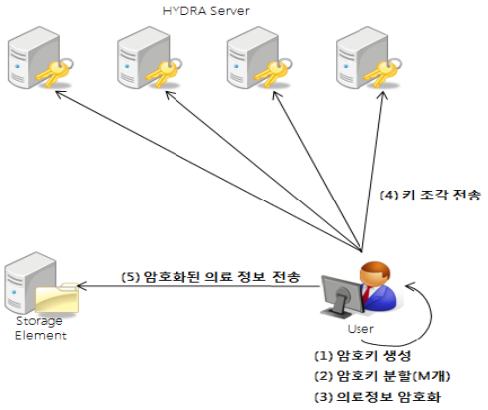
이 논문의 구성은 2장에서는 관련연구로 PHR의 필요성과 문제점을 간략히 기술한다. 3장에서는 이 논문에서 제안하는 PHR의 프라이버시를 보장하는 키 분배 프로토콜을 제안하고 평가한다. 마지막으로 4장에서는 결론으로 구성한다.

## II. 관련연구

기존 의료정보의 보안을 위해 다양한 방법의 논문들이 제시되고 있다. 의료정보 데이터의 보안을 위해 데이터암호화를 위한 분산 암호화 방법으로 [2]의 분산키 관리 HYDRA가 제안되었다. HYDRA는 데이터를 보호하기 위해서 의료정보관리 서비스에서는 DICOM 서버에 의료정보를 저장할 때 암호화 하게 되는데 이런 경우 외부의 공격자나 내부의 비인가 사용자가 의료정보를 획득하는 경우 내용을 복호화 할 수 없도록 키를 분산 관리하는 방법으로 제안되었다.

HYDRA는 암호키 관리 측면에서는 우수하지만 분산으로 저장되는 암호키 조각 보안에 있어서는 문제점을 갖는다. HYDRA서버는 키 조작을 요청하는 사용자를 인증하여 정당한 사용자로 확인되면 키 조각을 전송한다. 그러나 그림1에서와 같이 사용자에 의해서 분리된 키 조각은HYDRA 키 서버로 전송되는데 전송경로에 대한 안전성이 보장되지 않는다. HYDRA서버와 DICOM 클라이언트는 평문 형태의 키 조각을 교환한다.

따라서 공격자는 HYDRA서버와 DICOM 클라이언트 사이의 통신 내용을 도청하여 키 조각을 획득할 수 있다는 문제점을 갖는다.




[그림 1] HYDRA의 암호키 저장과정

[3]은 u-헬스케어에서의 분산데이터 접근방법을 제안한 논문으로 환자의 의료건강정보를 제 3자가 불법적으로 접근하지 못하도록 사용자의 식별체계를 활용한 사용자 프라이버시 보호 모델이다. 그러나 [3]의 논문은 개인의 의료정보측면에서 매우 협소한 정보만을 다루고 있고 체내 삽입장치를 부착한 환자의 프라이버시 보호만을 다루고 있어 기존 PHR에 적용하기에는 유연성이 매우 떨어지는 문제점을 갖는다.

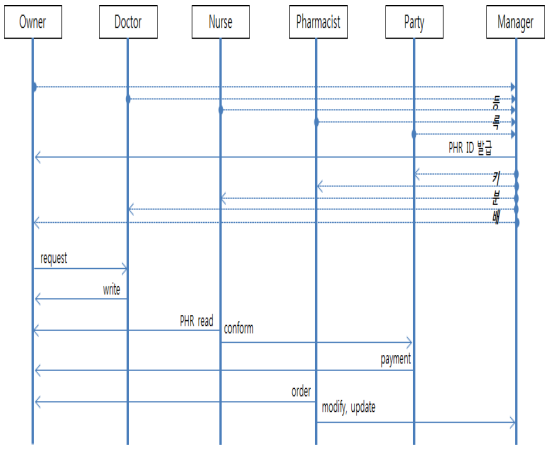
## III. PHR의 프라이버시 보호를 위한 키 분배 프로토콜

PHR은 의료정보 중 가장 프라이버시 보호가 필요한 정보 중 하나이며, 개인의 프라이버시에 대한 관심은 점차로 고조되고 있다. 진료기관에 노출된 PHR의 정보를 진료자의 역할에 따라 권한을 부하하고 권한별로 PHR의 접근을 허가한다. PHR에 접근하기 위해서는 먼저 PHR서버에 사용자 등록이 이루어져야하고 등록단계에서 자신에 맞는 역할이 선정된다. 역할은 표1과 같이 정의한다.

[표 1] 역할구분

| 사용자 | 구분 | 역할 |
|---|---|---|
| 환자 | (Owner) | root |
| 의사 | (Doctor) | read, write |
| 간호사 | (Nurse) | read |
| 약사 | (Pharmacist) | order |
| 병원관계자 | (Party) | management, modify |
| 관리자 | (Manager) | authentication, read |

사용자별 권한설정은 인증기관에서 발급된 각 사용자의 고유번호를 기반으로 관리자가 생성한다. 사용자 등록이 이루어지면 사용자는 PHR접근에 사용될 키를 발급받고 PHR 접근에 관한 권한은 [그림 2]와 같이 발급받는다.




[그림 2] 역할 기반의 키분배 프로토콜

▶ 등록단계

자신의 아이디와 패스워드를 이용해 개인식별값(IV)를 계산한다. IV를 이용해 PHR 관리자에게 등록을 요청한다. 사용자는 자신들의 역할 값을 부여받기 위해 역할을 구분할 수 있는 고유

값들을 전달한다.

$$Owner: IV = [ID_i, h(r||PW_i), HN]$$
$$Doctor: IV = [ID_i, h(r||PW_i), DN]$$
$$Nrse: IV = [ID_i, h(r||PW_i), NN]$$
$$Phamacist: IV = [ID_i, h(r||PW_i), PN]$$
$$Party: IV = [ID_i, h(r||PW_i), CN]$$

관리자는 사용자의 등록 요청시 수신한 IV에서 유효한 ID인지를 확인하고 유용한 경우 사용될 개인키를 생성하여 전달한다. 관리자는 개인키 생성시 각 권한 값을 기준으로 개인키를 계층적으로 생성하고 전달한다.

생성된 개인키에 따라 레코드의 접근 권한이 달라지기 때문이다. 권한 값 계산은 환자는 ID⊕의료보험번호(HN), 의사는 ID⊕의사면허번호(DN), 간호사는 ID⊕간호사면허번호(NN), 약사는 ID⊕약사면허번호(PN), 병원관계자는 ID⊕주민번호⊙직급번호(CN)를 기분으로 역할 값을 생성한다.

$$Owner: N = N+1$$
$$PK_o = h(ID_i \oplus PW_i \oplus r)||T_i)$$
$$RK = h(ID_i||HN)$$
$$Doctor: N = N+1$$
$$PK_d = h(ID_i \oplus PW_i \oplus r)||T_i)$$
$$RK = h(ID_i||DN)$$
$$Nrse: N = N+1$$
$$PK_n = h(ID_i \oplus PW_i \oplus r)||T_i)$$
$$RK = h(ID_i||NN)$$
$$Phamacist: N = N+1$$
$$PK_p = h(ID_i \oplus PW_i \oplus r)||T_i)$$
$$RK = h(ID_i||PN)$$
$$Party: N = N+1$$
$$PK_c = h(ID_i \oplus PW_i \oplus r)||T_i)$$
$$RK = h(ID_i||CN)$$

이렇게 생성된 각 개인 키과 역할 키를 이용해 PHR에 대한 접근을 통제할 수 있다. 생성된 개인키와 역할 키를 주지적으로 갱신된다. 관리자는 키 갱신을 통해 키의 신뢰성을 높이고 직급변화에 따른 권한을 유동적으로 관리한다. PHR의 접근 권한은 기본적으로 관리자가 기본값을 정하지만 소유자별로 자신의 PHR 정보 공개여부를 선택하여 제공할 수도 있다.

## Ⅳ. 결 론

PHR은 평생 건강관리를 지원하기 위해 소비자에게 자신의 진료저오를 언제 어디서나 열람할수 있고 건강 정보를 직접 입력 및 관리할수 있도록 도와준 서비스이다. 이런 PHR은 우리가 지향하는 u-헬스케어 서비스의 초석으로 언제 · 어디서 · 누가 · 누구의 어느 의료정보에 어떻게 접근했는지 정확하게 관리되어야 하고 접근에 관한 추적성이 확보되어야 한다. PHR에 저장된 진료정보의 검색 및 이용시스템은 접근이력 정보 및 보안정책에 근거한 접근제어나 익명성을 제공하면서 검색을 허가해야 한다. 그렇지만 진료 업무에서 진료정보에 대한 접근권한과 임상연구, 교육업무 등을 위한 진료정보의 접근권한은 비록 동일직원의 동일 환자정보에 대한 접근일 경우라도 달라질 수 있기 때문이다. 따라서 제안 논문에서는 PHR에 접근하는 사용자에 따라 접근권한을 부여하기 사용자를 구분하고 역할을 구분하였다. 각 역할에 따라 권한값을 생성하고 권한값에 따라 PHR레코드에 접근을 제한한다. 의료데이터의 접근성을 개선하고 직원의 다양한 역할과 그 이력에 따른 접근제어를 유지할 수 있는 접근 권한관리방식, 프라이버시 보호 및 데이터 보안 메커니즘으로 활용이 가능하다.

## 참고문헌


[1] 송지은, 김신효, 정명애, 정교일, “u-헬스케어 서비스에서의 의료정보보호”, 한국정보보호학회, 정보보호학회지 제17권 제1호 pp. 47~56, 2007.

[2] Joni Hahkala, John White, Ákos Frohner, Kalle Happonen, “Distributed Key Management system For Sensitive Data”,ISGC’10, Taipei, Taiwan, 2010.

[3] 정윤수, 이상화, “ 유헬스케어에서의 환자의 프라이버시 보호방안 연구”, 정보보호학회, 정보보호학회논문지 제22권 제 4호, pp913-921, 2012.

[4] 이종후, 유진승, 윤희준, 장행진, “의료정보 보호를 위한 분산 키 관리 시스템 설계”, 한국인터넷 정보학회 학술대회, pp 429-434, 2010.

[5] Jiang Q, Ma J, Ma Z, Li G. “A privacy enhanced authentication scheme for telecare medical information systems”, Journal of Medical Systems, Volume 36, Issue 3, pp 1529-1535, 2012.

[6] Kumar, P.; Lee, S.-G.; Lee, H.-J. E-SAP: Efficient-Strong Authentication Protocol for Healthcare Applications Using Wireless Medical Sensor Networks. Sensors 2012, 12, 1625-1647.