情報保護學會論文誌
第 22 卷 第 4 號, 2012. 8

유헬스케어에서 환자의 프라이버시 보호 방안 연구

정 윤 수,[1†] 이 상 호[2‡]
[1]목원대학교, [2]충북대학교

A Study of Patient's Privacy Protection in U-Healthcare

Yoon-Su Jeong,[1†] Sang-Ho Lee[2‡]
[1]Mokwon University, [2]Chungbuk National University

요 약

유헬스케어 서비스의 급속한 발전과 보급에 힘입어 유헬스케어 서비스 기술은 많은 변화가 이루어지고 있다. 그러나 유헬스케어 서비스는 보안상의 문제로 인하여 사용자의 민감한 의료정보가 제3자에게 유출되고 사용자의 프라이버시가 사용자의 동의없이 침해되는 문제가 발생되고 있다. 본 논문에서는 유헬스케어 환경에서 사용되고 있는 환자의 프라이버시 정보에 안전하게 접근하기 위해서 병원관계자의 권한 및 접근 레벨에 따라 환자의 생체정보를 분산 접근하는 모델을 제안한다. 제안 모델은 환자의 생체정보의 접근을 제어하는 동시에 타임스탬프를 통해 DoS 공격 예방과 최신성을 유지한다. 또한, 제안 모델은 병원관계자를 중앙에서 서버가 통합 관리하는 동시에 병원마다 병원관계자의 권한 및 레벨에 따라 접근을 제어하기 때문에 환자의 프라이버시 침해 및 의료정보 유출을 예방한다.

ABSTRACT

On the strength of the rapid development and propagation of U-healthcare service, the service technologies are full of important changes. However, U-healthcare service has security problem that patient's biometric information can be easily exposed to the third party without service users' consent. This paper proposes a distributed model according authority and access level of hospital officials in order to safely access patients' private information in u-Healthcare Environment. Proposed model can both limit the access to patients' biometric information and keep safe system from DoS attack using time stamp. Also, it can prevent patients' data spill and privacy intrusion because the main server simultaneously controls hospital officials and the access by the access range of officials from each hospital.

Keywords: Cloud Computing, User Authentication Protocol, Distribution Process, Certification

I. 서 론

유헬스케어 서비스는 인간의 건강회복, 유지 및 증진을 위해 언제 어디서나 의료서비스를 이용할 수 있도록 IT를 토대로 제공되기 때문에 최근 각광을 받고 있다. 유헬스케어 서비스는 건강진단이나 질병관리, 응급관리, 의사와의 만남 등 그동안 병원에서만 이루어지던 행위가 보다 편리한 형태로 사용자에게 제공되는 서비스이다[1].

유헬스케어 서비스의 모델은 크게 의료기관 중심의 유헬스 모델과 이용자 중심의 유헬스 모델(홈 헬스케어)이 있다. 의료기관 중심의 유헬스 모델은 의료기관의 내부 또는 의료기관 간에 진료 업무의 효율화를 증대시키기 위한 서비스 모델이며, 이용자 중심의 유헬스모델(홈 헬스케어)은 의료기관 외부의 이용자와 의료진을 연결하여 진료의 효율화를 증대시키기 위한 서비스 모델이다. 이용자 중심의 유헬스케어시스템의 주요 역할은 주로 만성질환자 또는 건강위험자를 대상으

접수일(2012년 3월 6일), 수정일(1차: 2012년 4월 18일, 2차: 2012년 7월 4일), 게재확정일(2012년 7월 22일)
† 주저자, bukmunro@mokwon.ac.kr
‡ 교신저자, shlee@cbnu.ac.kr

〔표 1〕 국내 홈&모바일 헬스케어 시장 규모

만성질환병명	시장규모(억원)	주요 측정 및 서비스 항목
고혈압	6,926	혈압, 체중
당뇨	2,741	혈당, 혈압, 체중
천식	1,545	호흡, 폐기능, 체중
심혈관질환	874	심전도, 심박, 혈압
소계	12,086	
관절염	5,470	재활 및 약물상담
고지혈증	1,363	혈액, 식이상담
뇌졸증	766	재활 및 간병인서비스
소계	7,599	
합계	19,685	

참조 : 삼성경제연구소

로 의료진의 적절한 개입(Intervention)과 이를 수행하고 만성질환자 또는 건강위험자의 충실한 이행도(Compliance)를 향상하도록 정보를 제공하는데 목적이 있다.

〔표 1〕은 국내 홈&모바일 헬스케어 시장규모를 나타내고 있으며, 국내 홈&모바일 헬스케어군은 2012년 최소 2조원 시장이 예상되는 가운데, 다양한 분야의 헬스케어 산업이 발전될 전망이다. 통신기술 발달과 함께 등장한 유-헬스케어는 만성질환을 앓는 고령인구가 많고 유비쿼터스와 원격의료 기술이 발달한 선진국이 연구 개발을 주도하여 왔다. 한국은 2005년 11월 유비쿼터스 시스템 구축을 마친 연세대학교 세브란스병원을 비롯하여 주로 대학병원들을 중심으로 도입 사례가 확대되는 추세이다. 유헬스케어사업단을 구성한 고려대학교의료원은 2006년 4월부터 서울 성북구보건소와 공동으로 성북구지역의 만성질병환자와 독거노인 등을 대상으로 시범사업을 벌이고 있다〔2,3,4,5〕.

유헬스케어 서비스는 현재까지 사용자의 정보를 개인이 관리할 수 있도록 개인정보 자기 통제권 확보 기술과 개인정보를 전송하고자 하는 대상자만이 해설할 수 있도록 암호화하는 방법 및 정보 활용시 개인 정보를 통해 개인을 식별하지 못하도록 하는 익명화 방법 중심으로 연구되어 왔다〔6,7〕. 그러나, 유헬스케어 서비스는 의료 정보 서비스 확대 및 의료 도메인간의 데이터 교환 상호 호환성을 위한 환경으로 변화하고 있다. 유헬스케어 서비스 환경에서 사용자의 개인정보를 다수의 병원에서 보장받기 위해서는 이질적 의료 도메인 간 개인의 건강/의료 정보를 교환 시, 인증된 도메인 간에 안전하게 가용한 정보만을 송・수신하도록 지원할 수 있는 보안 기술 및 모델이 필요하다.

본 논문에서는 서로 다른 유헬스케어 서비스 공간에서 환자의 의료 건강 정보를 제 3자가 불법적으로 접급하지 못하도록 사용자의 식별체계를 활용한 사용자 프라이버시를 보호 모델을 제안한다. 제안 모델은 병원마다 서로 다른 환자 식별 체계를 사용하여 환자의 생체정보에 접근하려는 문제점을 중앙의 서버가 단계별 병원관계자를 접근제어하여 환자의 프라이버시를 보호한다. 또한 병원간 건강/의료 정보를 공유할 경우 제안 모델은 불필요한 개인 정보의 노출 없이 익명성을 보장받도록 병원관계자의 권한을 분산 처리하여 환자 정보에 접근하도록 병원관계자의 권한을 제한한다.

이 논문의 구성은 다음과 같다. 2장에서는 유헬스케어 서비스 개념과 요구사항에 대해서 알아본다. 3장에서는 병원관계자의 불법적인 개입없이 병원 및 병원간 환자의 정보를 활용할 수 있는 사용자 프라이버시 보호 모델을 제안하고, 4장에서는 제안된 모델의 보안 평가를 분석하고 마지막으로 5장에서 결론을 맺는다.

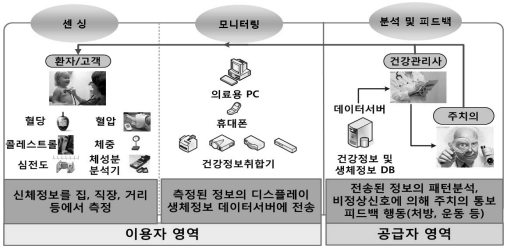
II. 관련연구

2.1 유헬스케어 서비스

유헬스케어 서비스는 홈네트워크 상의 장치나 휴대용 장치 등의 정보통신기술이 의료와 접목되어 생체정보를 실시간으로 모니터링하고 자동으로 병원 및 의사와 연결되어 시간과 공간에 구애 받지 않고 언제 어디서나 건강을 관리하고 증진시키며 질병을 예방하고 관리하는 새로운 형태의 의료 서비스를 의미한다

〔1,8〕. 유헬스케어는 의료기관 내 영역, 의료기관과 의료기관 사이 영역, 의료기관과 개인 사이에서 건강관리 관련 정보 및 서비스를 제공하는 영역 등으로 서비스를 구분하고 있다. 유헬스케어는 과거 전통적인 헬스케어의 영역에서 물리적, 시간적으로 제약되어 있던 서비스의 편리성을 높이기 위해 유·무선 온라인 네트워크를 활용하여 전자적 의료정보 및 진료 예약관리 등을 제공하던 e-헬스케어 단계에서 한단계 더 진화된 서비스이다〔1〕.

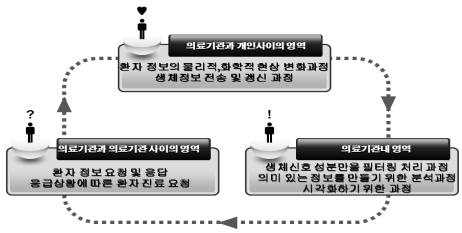
〔그림 1〕은 유헬스케어 서비스에 대한 개념도이다. 〔그림 1〕에서 유헬스케어 서비스는 센싱, 모니터링, 분석 및 피드백으로 구성된다. 센싱은 인체에서 발생하는 물리적·화학적인 현상의 변화를 감지하여 처리 가능한 전기적 신호로 변환하는 곳이며, 모니터링은 측정된 생체정보를 의미 있는 생체신호 성분만을 선택하기 위한 필터링 처리와 의미 있는 정보로 만들기 위한 분석과정, 그리고 이를 시각화하기 위한 과정으로 구성된다.



〔그림 1〕 유헬스케어 서비스 개념도〔11〕

〔그림 1〕에서 분석은 단순히 현재의 상태를 모니터링 할 뿐만 아니라, 장 시간에 걸쳐 측정된 데이터로부터 건강상태, 생활패턴 등을 나타내는 새로운 건강자료를 분석하는 과정이고 피드백은 장시간에 걸쳐 파악된 건강 기지선이나 생활의 변화를 사용자의 행동변화, 경고 등으로 사용자에게 제공하는 과정이다.

〔그림 2〕는 유헬스케어 환경의 의료기관내 정보 분산 처리 흐름을 나타내고 있다. 〔그림 2〕처럼 의료기관내 정보 분산 처리 흐름은 의료기관과 개인사이의 영역, 의료기관내 영역, 의료기관과 의료기관 사이의 영역 등 3가지 영역으로 구분된다. 의료기관과 개인사이의 영역에서는 인체에서 발생하는 물리적·화학적인 현상의 변화를 감지하여 처리 가능한 전기적 신호로 변환하거나 변경된 생체정보를 갱신한다. 의료기관내 영역에서는 인체로부터 모니터링된 측정된 생체정보를 의미 있는 생체신호 성분만을 선택하기 위한 필터링 처리와 의미 있는 정보로 만들기 위한 분석과정, 그리고 이를 시각화하기 위한 과정을 수행한다. 마지막으로 의료기관과 의료기관 사이의 영역에서는 환자의 응급상황이나 타병원 진료 요청에 대해서 환자의 상태를 모니터링하거나 장 시간에 측정된 데이터로부터 건강상태, 생활패턴 등의 새로운 건강자료를 관리한다.



〔그림 2〕 유헬스케어 의료기관내 정보 분산 처리

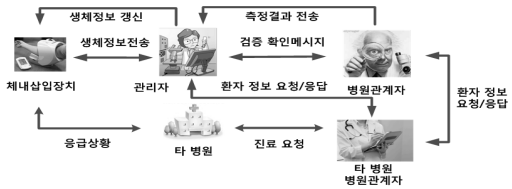
2.2 유헬스케어 보안 요구사항

2.2.1 ine-grained 데이터 액세스 제어

환자의 개인 정보가 제3자에게 노출되지 않기 위해서는 환자 데이터에 대한 접근제어를 강화할 필요가 있다〔9,10〕. Fine-grained 액세스 정책은 서로 다른 사용자를 위해 서로 다른 액세스 권한을 명세화하거나 강화되는 것을 정의하고 있다. Fine-grained는 환자의 관련된 데이터나 사용자 역할 사이에 구분되는 데이터 액세스 정책의 작은 부분까지 참조할 수 있다. 유헬스케어 시스템에서는 데이터에 대한 접근권한이 있더라도 사용자의 상황에 따라 접근이 제한될 수 있다. 예를들어, 사용자가 환자에 대한 건강 정보를 읽을 수 있는 권한이 있을 때, 사용자는 문맥을 고려하여 환자의 건강정보를 읽을 수 도 있고 읽지 못할 수 도 있는 상황이 발생할 수 있다.

2.2.2 확장성

환자와 관련된 데이터가 많을 경우 분산 액세스 제어 메커니즘은 쉽게 설정하고 수정될 수 있는 액세스 정책의 낮은 관리 오버헤드, 낮은 계산량과 저장 오버헤드 측면에서 많은 환자 정보와 함께 확장되어야 한다. 최근 스마트폰을 이용한 IT 의료 어플리케이션 개발이 다방면에서 연구되고 있다〔11,12〕. 이러한 연구는 스마트폰이 유헬스케어 기기의 활용으로 주변의 온도나 사용자의 체온 등을 측정하여 사용자 주변의 환



〔그림 3〕 사용자 프라이버시 보장을 위한 제안 모델

경 변화를 관찰할 수 있기 때문이다. 스마트폰을 이용한 헬스케어는 모바일 환경을 더욱 적극적으로 활용할 것이며 응용 범위를 더 넓혀 응급의료, 원격 진료 등에서 사용할 것이다.

2.2.3 유연성

유헬스케어의 기본 요구사항은 환자 자신의 데이터가 애플리케이션 및 모든 응용 프로그램의 외부 사용자 요구 사항에 대해서 유연해야 한다. 특히, 애플리케이션이 환자와 관련된 시간, 위치 등 특정 이벤트처럼 문맥에 동적으로 적용되는 것이 중요하다. 예를 들어 환자의 모니터링 데이터를 읽기 위한 온디멘드(on-demand) 권한은 응급상황이 발생했을 때 허락된 리스트에 없는 이용가능한 의사가 임시적으로 주어질 수 있다. 유헬스케어 환경에서는 동일한 사용자 할지라도 사용자가 자원에 접근하고자 하는 위치에 따라 다른 접근 권한이 필요하기 때문에 〔13〕에서는 위임 정책을 제공하여 사용자의 위치정보에 따라 역할이 활성화되는 연구를 하였다.

2.3 유헬스케어 사례

삼성의 의료기기 사업은 삼성전자와 삼성의료원을 주축으로 현재 추진 중이며, 기업인수합병(M&A)를 통해 빠르게 조직의 규모와 경쟁력을 확보해 가고 있다. 2010년에 국내 엑스레이기기 제조업체 레이 사와 초음파기기 업체 메디슨 사를 인수한 데 이어 지난해 11월에는 심장질환 검사기기 업체인 미국의 넥서스 사를 인수하여 X선으로 얻어진 영상을 디지털 데이터로 바로 저장하고, 의료용 디지털 영상·통신(DICOM) 표준에 따라 PACS 서버로 전송할 수 있는 기능을 갖춘 의료기기 개발하였다. 현대중공업과 SK 케미칼은 수술로봇의 수요가 많은 우리나라는 인공관절 수술로봇을 비롯한 모든 의료용 로봇을 전량 수입에 의존해 국산화의 필요성이 지속적으로 제기되어 지식경제부 국책과제인 '인공관절 수술로봇의 국산화 개발'에서 수술로봇 본체와 제어기 등 핵심장치를 개발하였다.

III. 유헬스케어에서의 분산 데이터 접근 제어 모델 설계

유헬스케어 환경에서 체내삽입장치를 부착한 환자의 프라이버시를 보호하기 위해서 병원관계자의 속성값의 권한을 분류하여 분산된 환자 데이터에 대한 접근을 제어하여 체내삽입장치를 사용한 환자의 프라이버시를 보호하기 위한 제안 모델은 그림 3과 같다. 〔그림 3〕의 제안 모델에서는 기존의 속성기반 암호 시스템의 특성을 적용하여 초기화 단계, 상호 인증 단계 그리고 복구 및 조회 단계 등이 동작된다. 기존 연구에서는 타 병원관계자가 환자의 생체정보를 관리하는 관리자에게 환자의 생체정보를 요청할 경우 병원 관계자와 타 병원 관계자 사이에 환자 정보 요청/응답 없이도 환자의 생체정보 전달이 이루어졌지만 제안 모델에서는 타 병원 관계자와 병원관계자 사이에 환자 정보 요청/응답을 통해서만이 환자의 생체정보를 타 병원 관계자에게 전달할 수 있다. 이 때, 관리자는 병원관계자와 타 병원 관계자의 신원을 타 병원 관리자에게 요청하여 인증된 경우에만 환자의 생체정보를 전달하여 응급상황이 발생한 환자를 진료할 수 있다.

초기화 단계에서는 환자의 생체정보를 진찰 및 측정하기 위해서 병원관계자의 속성에 따라 속성값과 비밀값으로 이루어진 비밀정보를 할당받는다. 병원관계자는 역할과 기능에 따라 여러 속성들을 갖고, 특정 환자의 생체정보에 접근하고자 할 때 병원관계자의 모든 속성이 적용되거나 접근레벨에 따라 병원관계자의 일부 속성만을 적용한다. 병원관계자의 모든 권한 속성을 $P_i=\{P_1, P_2, \ldots, P_n\}$라고 가정할 때, 병원관계자의 모든 원소가 인증과정에 필요하거나 병원관계자의 일부 권한 속성 $\{P_1, P_2, \ldots, P_k\} \subseteq P_i$ $(k \leq n)$만이 인증과정에 사용된다. 여기에서 k개의 권한 속성은 전체 n개의 권한 속성 중에서 임의로 선택된 것을 의미한다.

상호 인증 단계에서는 인증서버가 병원관계자의 권한 속성(소속부서, 직급, 역할 등)에 따라 환자의 생체정보에 접근하는 병원관계자들을 인증하고 환자에게 제공되는 서비스의 특성 값을 통해 환자의 생체정보를 안전하게 갱신한다. 복구 및 조회 단계는 환자가 응급상황이 발생하여 타 병원에 진료 요청을 할 경우 타 병원 관계자가 환자의 담당 병원관계자나 관리자에

게 환자 정보를 요청하고 응답하는 단계이다. 그림 4에서 관리자는 체내상입장치를 부착한 환자를 관리하기 위한 병원관계자의 정보(이름, 사번, 주민번호 등)를 바탕으로 병원관계자의 속성(해당부서, 직급, 역할 등)을 확인하고 병원관계자의 속성집합 $P_i=\{P_1, P_2, \ldots, P_n\}$을 결정하는 역할을 수행한다.

3.1 분산된 환자 정보 접근 제어

제안 모델은 분산처리기법을 이용하여 환자의 신분 및 인증을 병원관계자(의사, 간호사, 약사 등)의 권한 속성 정보를 바탕으로 처리되며, 분산된 환자 정보의 접근 제어는 초기화 단계, 인증 단계, 병원 관계자의 권한정보 복구 및 조회 단계 등의 3단계로 구성된다.

3.1.1 초기화 단계

초기화 단계에서는 분산된 환자 정보에 접근하기 위해서 병원관계자의 정보(해당부서, 직급, 역할, 사번, 주민번호 등)와 아이디 ID_U, 패스워드 Pw_U를 인증서버에 보낸다. 인증 서버는 병원관계자의 정보를 이용하여 속성 집합 $P_i=\{P_1, P_2, \ldots, P_n\}$를 결정하여 인증 서버의 비밀키 S_k와 함께 식 (1)을 계산한다.

$$X_i = h(ID_U, Pw_U) \oplus h(P_i \oplus S_k) \quad (1)$$

인증 서버는 식 (1)을 인증서에 저장하여 관리자에게 전달한다. 제안 모델에서는 병원관계자의 속성 정보가 저장된 인증서를 PKI를 통해 환자의 생체 정보에 접근 처리할 수 있도록 한다. 초기화 단계에서 이같이 처리하는 이유는 관리자가 병원관계자의 속성 인증서를 관리하여 속성에 따라 그룹을 할당하고 설정된 정책과 속성정보를 가지고 권한을 부여하여 접근제어가 이루어지게 하기 위해서이다.

3.1.2 인증 단계

인증 단계에서는 병원관계자의 속성과 타임스탬프에 따라 환자 정보에 접근하는 병원관계자를 제어하는 단계이다.

• 1단계

병원관계자의 권한 속성 정보를 식 (2)~식 (3)의 과정을 통해 추출한 후 병원관계자의 권한을 인증 서버에 요청하여 응답을 기다린다.

$$M_l=\{M_l \mid M_l \in M,\ 1 \le l \le L\} \quad (2)$$
$$m_l = C(M_l) \quad (3)$$

여기서 L은 분산된 병원관계자 정보의 총 개수를 의미한다. 단, M은 $M_1 \cup M_2 \cup \cdots \cup M_L$이고 $\varnothing = M_1 \cap M_2 \cap \cdots \cap M_L$ 이라고 가정한다.

• 2단계

인증서버는 병원관계자에게 권한 정보를 보내기 위해서 소수 $q(q \ge n+1)$를 선택한 후 Z_q에서 임의의 랜덤 수 $a_i(1 \le i \langle t)$를 선택하여 이진수 k로 변환한다. 변환된 이진수 k를 상수항으로 하는 임의의 다항식 $a_{(n-1)(k-1)}+a_{(n-1)k}$이 생성되면 식 (4)처럼 다항식을 a_{nk}로 변환하여 타임스탬프와 함께 관리자에게 전달한다. 여기서, 다항식 $a_{(n-1)(k-1)}+a_{(n-1)k}$은 병원관계자의 권한 정보를 트리구조의 계층적 형태로 정보를 생성한다.

$$a_{nk} = a_{(n-1)(k-1)} + a_{(n-1)k} \ (n,k \rangle 1) \quad (4)$$

• 3단계

관리자는 인증서버로부터 전달받은 병원관계자의 권한 정보 a_{nk}가 n 번째 줄의 k 번째 값이라고 하면, 이 값은 식 (5)~식 (7)처럼 정의할 수 있다.

$$a_{n1} = 1 \quad (5)$$
$$a_{nn} = 1 \quad (6)$$
$$a_{nk} = a_{(n-1)(k-1)} + a_{(n-1)k} \ (n,k \rangle 1) \quad (7)$$

이 때, 식 (8)과 같은 다항식의 성질을 이용하여 식 (9)처럼 병원관계자의 속성 정보값을 추출한다.

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \quad (8)$$
$$a_{nk} = \binom{n-1}{k-1} \quad (9)$$

즉, n번째 열의 k번째 값은 $\binom{n-1}{k-1}$과 같은 병원관계자의 권한 정보값으로 구해진다. 관리자는 병원관계자의 권한 정보에 따른 환자의 생체정보를 병원관계자에게 전달한다.

3.1.3 병원 관계자의 권한정보 복구 및 조회

병원 관계자의 권한 정보 복구 및 조회에서는 최소 n 명이상의 병원 관계자에 대해서 a_{nk}를 수집하여 인증서버에 보관되어 있는 다항식 $a_{(n-1)(k-1)}+a_{(n-1)k}$의 계수를 찾는다. 병원관계자의 권한정보를 복구 및 조회하기 위해서는 a_i와 x_j을 식 (10)처럼 복원하거나 행렬식으로 해를 구한다.

$$(x+y)^n = a_0x^n + a_1x^{n-1}y^1 + a_2x^{n-2}y^2 + \cdots + a_ny^n \quad (10)$$

식 (10)은 전개되면 $a_i = \binom{n}{i}$와 같은 식이 성립한다. 즉, a_i는 $(n+1)$번째 줄의 $(i+1)$번째 값과 대응된다. 병원관계자의 개인 정보 M_l는 모든 l에 대해서 반복적으로 $m_l = C^{-1}(M_l)$ 형태로 변환 작업을 수행하고, m_l을 $M = M_1 \cup M_2 \cup \cdots \cup M_L$으로 만들어 환자의 개인정보를 복구 및 조회한다.

3.2 권한확인 및 제어

제안 모델에서는 병원관계자의 권한에 따라 역할을 제한한다. 이때 부여된 권한은 역할기반의 접근제어를 사용하며, 병원 관계자의 역할은 의료 업무에 따라 분류한다. [표 2]은 제안 모델에서 권한 확인 및 제어를 위해 역할기반의 접근제어에서 사용되는 구성요소들이며 각 구성요소의 역할을 정의하고 있다. 제안 모델은 병원관계자의 권한을 통해 병원관계자의 임무분리와 최소권한을 부여하여 환자의 개인 정보 유출 및 진료 정보의 손실을 예방하고, 권한 없는 제3자의 정보 접근을 제어한다.

IV. 보안평가

본 절에서는 유헬스케어 서비스에서 요구되는 보안 요구사항을 기반으로 제안기법의 안전성을 평가한다.

4.1 내부보안

4.1.1 사용자 인증

병원관계자는 사용자 인증을 수행하기 전에 인증서버에 등록해야 하고 관리자는 인증서버에 등록된 병원관계자의 권한 정보를 확인한 후 관리자는 병원 관계자의 권한 정보를 이용하여 병원관계자의 권한 등급에 따른 환자의 생체정보의 접근을 허가한다. 병원관계자의 권한 정보 a_{nk}는 환자와 병원관계자 사이에 환자의 생체 정보를 안전하게 전달하기 위한 인증 수행을 처리하기 위한 과정으로써 관리자는 공개키 암호 알고리즘을 사용하여 인증을 수행하고 병원관계자의 권한 정보 a_{nk}에 따른 접근을 엄격하게 제약한다.

4.1.2 사용자 프라이버시

환자의 프라이버시를 보호하기 위해서 환자의 생체정보에 접근하는 병원관계자의 권한 정보를 인증서버에 사전에 등록한 후 인증서버에 등록된 병원관계자의 권한정보에 따라 관리자는 환자의 생체정보의 접근제어를 제어한다. 이 때, 생체정보의 접근은 접근레벨에

[표 2] 구성요소

요소	설 명
사용자	내부삽입장치를 부착한 사용자
역할	의료 업무의 책임과 권한에 관련된 의료 조직 내 직함 -의사, 간호사, 환자, 약사 등
세션	동적으로 사용자와 역할을 할당할 수 있도록 관리
동작	하나 혹은 그 이상의 보호된 RBAC 객체들 (환자의 개인정보)의 집합에 접근하기 위한 특정 접근 방식 -Read, Write, Delete 등
데이터	USHS 모델에 의해서 관리되는 대상이며 환자의 개인정보를 말함
목적	USHS 시스템에서 환자의 정보를 이용하려는 목적들을 정의 -처방, 진료 등
제약사항	사용자가 역할에 할당되는 조건, 역할 내 의료 업무의 제한조건, 정보의 이용에 필요한 제약조건 등
병원관계자	환자의 생체정보를 분석, 관찰하여 환자 상태를 관리하는 의사, 약사, 간호사 등을 말함
관리자	환자와 병원관계자를 인증하는 작업과 환자의 생체정보를 수집하여 최신의 상태를 유지하는 역할을 담당

따라 환자의 생체정보의 수집에 제한되기 때문에 환자의 프라이버시를 보장하고 있다. 특히, 병원관계자의 권한 정보를 임의의 다항식으로 만들어 관리자가 인증 서버로부터 전달받은 임의 상수 값으로 접근 권한을 만들기 때문에 기존 프라이버시 보호 기법보다 단순하면서도 효율적이다.

4.1.3 권한 정보의 최신성

환자의 생체 정보에 접근하는 병원관계자의 권한정보를 추출하기 위해서 타임스탬프 동안 관리자에게 병원관계자의 권한 정보를 유지하기 때문에 병원관계자의 권한 정보에 대한 최신성을 유지한다. 또한, 병원관계자의 권한 정보에 따른 접근 제어를 수행하기 때문에 환자의 생체정보의 최신성뿐만아니라 서비스 거부(DoS: denial of service) 공격을 방지한다.

4.1.4 액세스 권한 제약

관리자는 환자의 생체정보를 요청하는 병원관계자의 활동을 엄격하게 제약하기 위해서 병원관계자의 권한 등급에 따라 환자의 생체정보의 접근을 제약하고 있다. 제안 모델에서는 신분 및 인증을 병원관계자의 권한 속성 정보를 바탕으로 처리하기 때문에 병원관계자의 권한 속성 $P_i=\{P_1, P_2, \ldots, P_n\}$으로 환자의 생체정보 접근을 제어한다. 제안 모델에서는 2개 이상의 병원에서 환자의 생체정보를 요청할 경우 병원관계자의 권한 속성에 대한 정보를 모두 보유하여야 한다. 타 병원에서는 일정 시간 간격 사이로 권한 속성 정보가 변경될 수 있다. 제안 모델에서는 병원 H_i에서 병원 H_j로 환자의 생체정보 요청이 있을 경우 공개키로 암호화하고 복호화하는 과정이 홉-대-홉 방식으로 진행되기 때문에 Sybil 공격에 안전하다.

4.1.5 다단계 서비스 접근인증

병원관계자가 환자의 생체정보에 접근하기 위해서 접근권한에 따른 다단계 서비스 접근 인증을 수행하기 때문에 권한이 없는 병원관계자는 환자의 정보를 불법적으로 접근하지 못한다. 제안 모델에서는 접근권한에 따라 상호간 등록 및 인증 요청, 키 교환, 디바이스 인증 정보 전송, 인증 결과 전송 등이 완료된 후에만 서비스가 정상적으로 제공된다.

4.2 외부보안

4.2.1 Sybil 공격에 따른 보안

제안 모델은 환자의 생체정보를 병원관계자가 수집할 경우 무선 네트워크에서 임무를 수행하는 여러 환자들의 정보를 합병하기 위해서 합법적인 인식자를 사용하여 위장하는 Sybil 공격이 발생 될 수 있다. 그러나 제안 모델에서는 인증 서버가 병원관계자의 정보를 이용하여 속성 집합 $P_i=\{P_1, P_2, \ldots, P_n\}$를 결정하여 인증 서버의 비밀키 S_k와 함께 환자의 생체정보에 접근하는 접근권한 정보를 관리함으로써 환자의 생체정보를 생성하여 홉-대-홉 방식으로 패킷을 확인해 나감으로써 Sybil 공격을 예방하게 된다.

4.2.2 전송되는 과정에서의 정보 공격에 따른 보안

병원관계자는 무선통신용 AP 또는 공유기를 통해 전달되는 환자의 생체 정보의 변화를 모니터링하고 요구사항에 따라 정보를 서버내의 데이터베이스에 저장하는 역할을 수행하지만 환자의 생체정보 수집 및 전송 범위가 제한적이기 때문에 서버로 전달중인 사용자 정보를 제3자가 악의적으로 이용할 수 있는 문제점이 있다. 제안 모델에서는 홉-대-홉 방식으로 환자를 인증하면서 병원 관계자의 정보를 서버가 분산 관리하기 때문에 인증 서버가 환자의 정보를 판독하는 동안 제3자가 방해하지 못한다.

4.2.3 Blackhole/Sinkhole 공격에 따른 보안

Blackhole/Sinkhole 공격에서는 악의적인 사용자가 플로딩 기반 프로토콜을 사용하는 통신 사이에 존재할 경우 패킷 패싱과 같은 공격을 할 수 있지만 이러한 공격은 서버로부터 멀리 떨어져 있는 환자에게만 영향을 미친다. 제안 기법에서는 일정 시간 간격으로 인증 서버가 병원관계자의 속성 정보를 갱신하기 때문에 접근 권한에 따라 환자의 생체정보를 수집한다.

V. 결 론

최근 체내삽입장치를 사용하는 환자가 증가하면서 환자의 프라이버시 피해가 증가하고 있어 병원관계자가 불법적으로 환자의 생체 정보를 악용하는 것을 예방하기 위한 보안 기술 및 모델이 필요하다. 본 논문

에서는 체내삽입장치를 사용하는 환자의 프라이버시를 보호하기 위한 권한 속성기반의 병원관계자 정보의 분산 모델을 제안하였다. 제안 모델은 실 환경에서 효과적으로 활용할 수 있도록 병원관계자의 권한 정보를 상태 및 접근 레벨에 따라 관리할 수 있도록 하였다. 또한, 환자의 생체정보를 관리자가 관리하는 동시에 병원간 공유되는 환자의 정보에 대해서 프라이버시를 보호하기 위해서 병원관계자의 권한 및 레벨에 따라 환자의 생체정보에 접근하도록 제어하여 제3자에 의한 환자의 프라이버시 침해를 예방하였다. 보안 평가에서는 체내삽입장치를 사용하는 환자에서 발생할 수 있는 가장 대표적인 공격유형으로 제안기법의 안전성을 평가한 결과, 기존 모델에서 제기되었던 다양한 보안 문제점이 개선된 결과를 얻을 수 있었다. 그러나 제안 모델은 이론적 측면에서 제3자에 의한 환자의 프라이버시를 침해를 예방하고 있지만 실제 환경에 적용하지 못하여서 제안 모델의 성능평가에 대한 객관적 도출이 이루어지지 못하였다. 향후 연구에서는 환자의 정보를 분산 저장하여 타 병원간 환자 정보를 효율적으로 사용할 수 있는 메커니즘을 연구하여 실제 환경에 적용할 계획이다.

참고문헌

〔1〕 송태민, 장상현, "u-Healthcare 이슈 및 연구동향," 한국보건사회연구원, 보건복지포럼, 통권 제171호, pp. 70-86, 2011년 1월.

〔2〕 김경진, 홍승필, "e-Healthcare 환경 내 개인정보 보호 모델," 한국인터넷정보학회논문지, 10(2), pp. 29-40, 2009년 4월.

〔3〕 D. G. Kim, I. G. Song, "Need and Development of u-Healthcare Service," Korean Society for Internet Information, Vol. 1, No. 3, pp. 9-17, Sep. 2009.

〔4〕 D. H. Sin, B. J. Han, H. J. Lee, H. C. Jung, "Analysis of Security Threat in u-Healthcare Service," The Korean Institute of Information Scientists and Engineers 2010 Conferences, Vol. 37, No. 1(D), pp. 52-55, Jun. 2010.

〔5〕 S. Y. Song, H. J. Hwang, "u-Healthcare Application Framework for Medical Gateway," Korean Society for Internet Information Conference, pp. 349-353, May. 2009.

〔6〕 IHE, http://www.himss.org.

〔7〕 ITI Technical Committee, "IHE Security-XDS as a Case Study," IHE, 2006.

〔8〕 J. E. Song, S. H. Kim, M. A. Chung, K. I. Chung, "Security Issues and Its Technology Trends in u-Healthcare," Electronics and Telecommunications Trend Analysis Vol. 22, No. 1, pp. 70-86, Feb. 2007.

〔9〕 Z. Omary, f. Mtenzi, B. Wu, C. O'Driscoll, "Accessing sensitive patient information in ubiquitous healthcare systems," 2010 International conference for internet Technology and Secured Transactions (ICITST), pp. 1-3, Nov. 2010.

〔10〕 D. W. Bang, J. S. Jeong, J. H. Lee, "An implementation of privacy security for PHR framework supporting u-healthcare service," 2010 6th International conference on Networked Computing(INC), pp. 1-4, May. 2010.

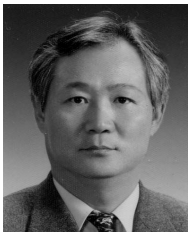
〔11〕 정윤수, 김용태, "아이핀 기반의 유헬스케어 사용자 정보 보호 프로토콜," 한국정보기술학회, 9(10), pp.133-141. 2011년 10월.

〔12〕 http://www.theMETATREND.com

〔13〕 이봉근, 정윤수, 이상호, "유헬스케어 서비스 환경을 위한 RBAC 기반의 프라이버시 모델," 한국정보기술학회, 9(9), pp. 105-116. 2011년 9월.

〈著者紹介〉

정 윤 수 (Yoon-Su Jeong) 정회원
1998년 2월: 청주대학교 전자계산학과 학사
2000년 2월: 충북대학교 대학원 전자계산학과 석사
2008년 2월: 충북대학교 대학원 전자계산학과 박사
2008년 3월~2009년 8월: 충북대 및 한남대 시간강사
2009년 9월~2012년 2월:한남대학교 산업기술연구소 전임연구원
2012년 3월~현재: 목원대학교 정보통신공학과 조교수
〈관심분야〉 정보보호, 멀티미디어, 네트워크 보안, 이동통신, 유·무선 통신, 암호이론



이 상 호 (Sang-Ho Lee) 정회원
1976년 2월: 숭실대학교 전자계산학과 학사
1981년 2월: 숭실대학교 대학원 전자계산학과 석사
1989년 2월: 숭실대학교 대학원 전자계산학과 박사
1981년 3월~현재: 충북대학교 전자정보대학 소프트웨어학과 교수
〈관심분야〉 네트워크보안, Protocol Engineering, Network Management