韓國컴퓨터情報學會 論文誌
第16卷 第11號, 2011. 11.

2011-16-11-4-2

유헬스케어 서비스 환경 내 개인정보 보호 모델 설계

이 봉 근*, 정 윤 수**, 이 상 호***

Design of Personal Information Security Model in U-Healthcare Service Environment

Bong-Keun Lee*, Yoon-Su Jeong **, Sang-Ho Lee ***

요 약

IT 기술의 급속한 발전과 보급에 힘입어 미래의 의료형태인 IT 융합 헬스케어 서비스 기술은 많은 변화가 이루어지고 있다. 특히, IT 기술이 헬스케어와 융합되면서 사용자의 민감한 의료정보가 유출되고 사용자 프라이버시가 침해되는 문제가 발생되면서 그에 따른 대비책이 필요하다. 본 논문에서는 유헬스케어 환경에서 사용자의 프라이버시를 보호하기 위해서 환자의 ID 정보를 사용자 상태 및 접근 레벨에 따라 통합/분할 관리할 수 있는 유헬스케어 서비스 모델을 제안한다. 제안된 모델은 실 환경에서 효과적으로 활용할 수 있도록 사용자 신분확인, 병원 권한확인, 진료기록 접근제어, 환자진단 등의 기능으로 구분한다. 또한, 사용자의 ID가 중앙의 서버에서 통합 관리되는 동시에 병원간 공유되는 사용자의 정보에 대한 프라이버시를 보호하기 위해서 사용자의 보안 레벨 및 권한에 따라 사용자의 ID를 병원에 분할 적용하여 제 3자에 의한 사용자의 프라이버시 침해 및 의료정보 유출을 예방한다.

▸ Keywords : 유헬스케어, 개인정보 보호, 역할기반

Abstract

With rapid development and contribution of IT technology IT fushion healthcare service which is a form of future care has been changed a lot. Specially, as IT technology unites with healthcare, because delicate personal medical information is exposed and user's privacy is invaded, we need preperation. In this paper, u-healthcare service model which can manage patient's ID information as user's condition and access level is proposed to protect user's privacy. The proposed model is distinguished by identification, certification of hospital, access control of medical record, and

• 제1저자 : 이봉근 • 교신저자 : 이상호
• 투고일 : 2011. 06. 01. 심사일 : 2011. 09. 05, 게재확정일 : 2011. 08. 25
* 부산경상대학 소방안전계열(Division of Fire Protection&Safety, College of Busan Kyungsang)
** 한남대학교 산업기술연구소 전임연구원(Industry Technical Research Institute, Hannam University)
*** 충북대학교 전자정보대학 소프트웨어학과 교수(Dep. Computer Science, College of Electrical & Computer Engineering, Chungbuk National University)

diagnosis of patient to utilize it efficiently in real life. Also, it prevents leak of medical record and invasion of privacy by others by adapting user's ID as divided by user's security level and authority to protect privacy on user's information shared by hospitals.

▸ Keyword : u-Healthcare, Privacy Protection, RBAC

Ⅰ. 서론

최근 의료 서비스 분야에 IT 기술이 적용되면서 다양한 종류의 소형, 휴대 가능한 장치들이 사용자의 건강상태를 모니터링하고 개인화된 건강관리 서비스를 제공하는 유헬스케어(u-Healthcare) 서비스가 각광을 받고 있다. 유헬스케어 서비스는 IT 기술과 선진의료기술이 결합된 고부가가치 융복합 산업으로 환자의 생체신호 및 건강 정보를 측정하고 유무선 네트워크를 통하여 데이터를 의료기관에 전송한 후 분석하고 다시 피드백 해줌으로서 환자의 질병에 대해서 원격관리뿐만 아니라 일반인의 건강관리가 가능할 수 있는 서비스이다[1].

기존 의료서비스에 유비쿼터스 기술을 접목하여 언제, 어디서나, 보건의료 서비스를 제공하고자 하는 유헬스케어 서비스의 경우 바이오정보를 포함한 개인정보와 의료정보를 다루기 때문에 해킹으로 인한 정보유출 사고발생시 국가적인 혼란과 사회적인 불신을 야기할 수 있는 문제점이 있다[2].

현재까지 연구된 유헬스케어 서비스의 개인정보보호 방법으로는 사용자의 개인정보를 자신의 통제 영역 안에 포함시켜 개인정보의 유통을 개인이 관리하도록 하는 개인정보 자기통제권 확보 기술과 개인정보를 전송하고자 하는 대상자만이 해석할 수 있도록 암호화하는 방법 및 정보 활용시 개인 정보를 통해 개인을 식별하지 못하도록 하는 익명화 방법이 있다[3,4,5].

유헬스케어 서비스에서는 타 유비쿼터스 컴퓨팅 기술 분야에 비해 정보 속성에 대해서 매우 민감하고 이질적인 서비스 도메인 간 혹은 다양한 서비스 관계자가 정보 공유가 빈번하게 이루어지기 때문에 불법적인 정보 노출 및 조작, 개인 프라이버시 침해 및 의료 서비스 위협 등과 같은 내·외부 보안 공격에 매우 취약하다.

ITI 기술 위원회에서 연구된 IHE-XDS은 유헬스케어 서비스의 대표적인 모델로써, 이 모델은 의료 데이터를 공유하는데 동의한 의료 도메인간에 데이터 교환 상호 호환성을 보장하고 데이터의 안전한 접근 및 활용을 보장하기 위해 교환할 환자/의료 데이터의 식별 방법과 메타 데이터 문서 구조 및 포맷, 인코딩/디코딩 규격 등에 관한 내용뿐만 아니라 데이터에 대한 접근 통제, 보안 감사 방법 등의 보안 기술을 제시하고 있다[6,7].

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 유헬스케어 서비스 환경에서 보다 향상된 수준의 의료 서비스와 개인의 의료 건강 정보에 대한 접근성을 용이하도록 환자의 건강 정보를 제3자가 안전하게 접근할 수 있는 유헬스케어 사용자 프라이버시 보호 서비스 모델을 제안한다. 제안 모델은 병원마다 서로 다른 환자 식별 체계가 사용되고 있는 병원에서 다양한 형태로 존재하는 다수의 ID 정보를 환자가 기억하지 않아도 인증되도록 중앙 서버가 집중 관리하는 동시에 병원 간 건강/의료 정보 공유시 불필요한 개인 정보 노출 없이 익명성을 보장받도록 ID 분산 처리기법을 사용하며 환자 정보에 대해서 환자 요청에 따라 서로 공유 및 활용 가능하도록 권한을 제한한다.

이 논문의 구성은 다음과 같다. 2장에서는 유헬스케어 서비스 개념과 보안 문제에 대해서 알아본다. 3장에서는 환자의 정보를 서로 공유 및 활용 가능한 분산/집중 혼합형 ID 관리 모델을 제안하고, 4장에서는 보안 공격에 따른 제안 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 생체 정보를 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 의료기관사이 영역, 의료기관과 개인 사이에서 건강관리 관련 정보 및 서비스를 제공하는 영역 등으로 서비스를 구분하고 있다. 유헬스케어는 과거 전통적인 헬스케어

의 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.

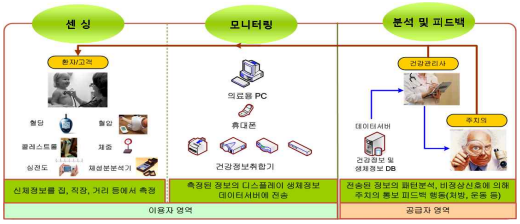


그림 1. 유헬스케어 서비스 개념도
Fig 1. u-Healthcre Service Design

[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]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.

2.2 유헬스케어 보안 문제

의료 서비스 기술이 발달함에 따라 유헬스케어의 의료정보 보안에 대한 요구가 급증하고 있으며, PKI 또는 데이터 암호화 등을 중심으로 보안 기술들을 제품에 적용하고 있다[8].

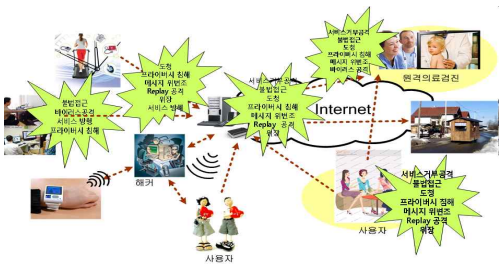


그림 2. 유헬스케어 환경의 보안 위협
Fig 2. Security Threat of u-Healthcre Environment

유헬스케어 환경에서 데이터 보호 및 프라이버시 보호 문제와 관련된 다양한 보안 취약점과 위협 요소들은 [그림 2]처럼 유·무선 네트워크 기반 서비스에서 발생 가능한 보안상 취약점과 유사하다. 그러나 유헬스케어 서비스는 기존 유·무선 네트워크 기반 서비스와는 다른 보안 요구사항들이 존재한다[9,10]. 유헬스케어에 사용되는 새로운 장비들과 네트워크상에서 존재하는 신규 취약점에는 첫째, 서비스를 지원하는 서버를 공격하는 DoS 공격 유형, 둘째, 바이러스/웜 해킹 공격 유형, 셋째, 의료정보 도청/위변조 공격 유형, 넷째, 유·무선 인프라에서 가능한 여러 불법 접근 공격 유형, 다섯째, 오프라인을 통한 방범 시스템 고장 및 인위적인 기기 마비, 방해전파, 화재와 같은 인재 또는 악의적인 행위를 통한 공격유형 등이 있다.

[그림 2]에서 유헬스케어 서비스의 주요 보안 위협은 Cart Rack 장비의 취약점을 이용하여 화상시스템에 직접 침투 또는 화상 전송되는 데이터를 도청 및 위·변조하는 화상시스템 해킹, 원격진료서비스, i-방문간호서비스, 재택건강관리서비스 등 유헬스케어 서비스에 대하여 허가받지 않은 사용자가 불법적인 침투을 시도하는 불법적인 접근, 무선 통신용 AP 또는 공유기의 무선망에 접근 및 불법 침투하는 무선 해킹, 불법적인 접근 시도 후, 전송되는 데이터를 도청 및 위·변조하는 도청/위변조, 의료장비에 백도어 또는 원격 터미널 클라이언트 등으로 권한을 획득하는 의료장비 해킹, 의료 지원용 홈페이지를 해킹하여 환장의 정보를 수집하는 웹 해킹, 웹과 연동되는 DB에 대하여 웹 로직의 SQL Injection 취약점을 이용하여 DB에 접근하여 내부 중요정보를 획득하는 개인 및 의료정보 DB 해킹, 웹 모의해킹 후, 웹 서버 권한을 획득 한 후, 연동된 내부망으로 2차 침투 시도를 하는 의료망 침투 등이 있다[7].

의료 서비스 정보는 환자가 이동함에 따라 중복된 검사와 의료 조치를 선택적으로 다른 의료 기관(병·의원 또는 보건소 등)에 위임할 때 개인 정보는 의료 서비스 목적에 맞게 최소한으로 공유할 수 있다. 그러나 현재 의료 정보 보안 정책 및 기술로는 그 범위를 명확하게 파악하거나 결정할 수 없는 문제가 있다. 또한 불법적인 의료 정보 열람과 이용을 막고 그 책임 소재를 판단하기 위한 보안 감사 체계가 보완되어야 한다. 대부분의 병원에서는 요청자의 단순 서비스 요청에 관한 로그만 남길 뿐, 데이터 습득 이후 활용, 폐기 등에 관한 의무사항 준수에 관련한 감사 체계가 부재하여 내부자에 의한 정보 유출의 위험성이 높다. 유헬스케어 환경에서는 ID/PW나 공인 인증서 기반뿐만 아니라 다양한 생체 식별 정보가 사용자 인증 방식으로 활용되지만 생체 정보는 그

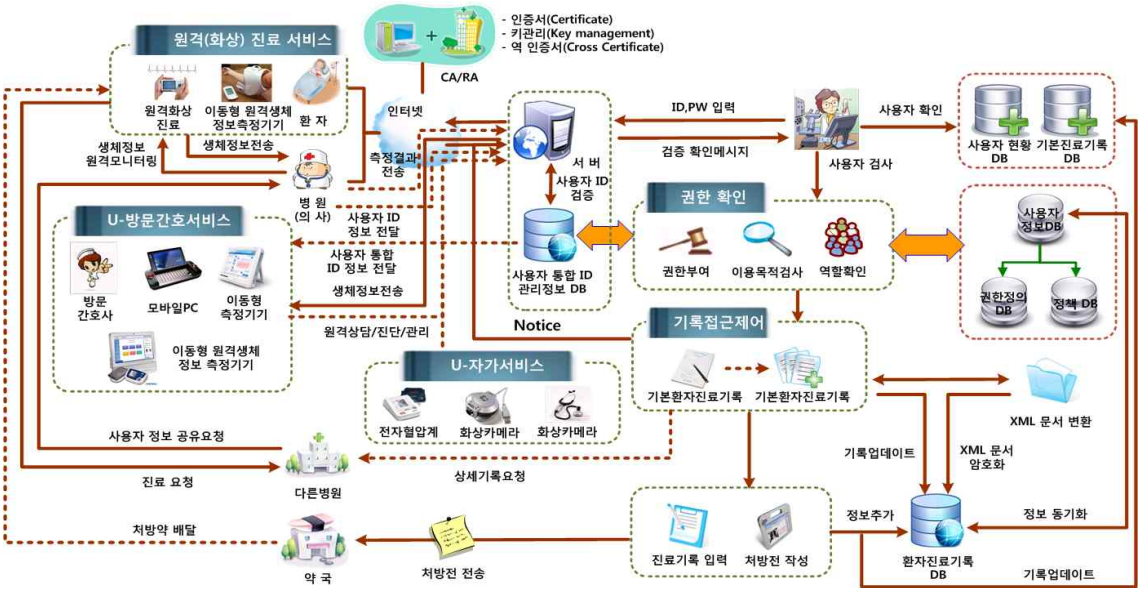


그림 3. 사용자 프라이버시 보장을 위한 제안 모델
Fig 3. Proposed Model for User Privacy Assurance

정보의 변경이 쉽지 않아 생체정보의 노출로 더 이상 사용이 불가능한 경우의 문제점이 발생할 수 있다.

2.3 기존 연구

유헬스케어 서비스에서 사용자 프라이버시 보호의 요구사항을 고려한 최근의 대표적인 모델 연구는 P-RBAC 모델[13,14], 목적기반 접근제어 모델[15], 상황 중심의 접근 모델[16] 등이 연구되고 있다.

P-RBAC 모델은 전통적인 RBAC에 프라이버시 정책들을 추가한 RBAC의 확장 모델이다[13,14]. P-RBAC 모델은 기존 RBAC 개념에 목적, 조건, 그리고 의무 사항이 추가되었으며 프라이버시 보호 요구사항 중 조건은 액션이 실행되기 전에 반드시 만족해야 조건이 있다. P-RBAC 모델은 프라이버시 퍼미션을 정의하여 프라이버시를 강화하는 장점은 있지만, 조건 표현이 풍부하지 못하고 목적 모델의 장점인 조건역할을 수용하지 못하는 단점이 있다.

목적기반 접근제어 모델은 사용목적 관리를 위한 사용목적 트리와 접근제어를 위한 RBAC의 역할계층 구조로 구분되며 계층구조로 사용목적을 관리하기 때문에 상위 목적은 하위 사용목적을 일반화하고, 하위 사용목적은 사용목적을 특수화한다. 목적기반 접근제어 모델은 사용목적의 중복성과 객체의 삽입·삭제 행위시 비일관성 문제를 해결할 수 있는 장점이 있으나 사용목적의 특성과 계층구조의 특성인 최상위 노드를 제외한 모든 노드들은 부모 노드를 가져야 한다는 제약 사항으로 인하여 문제점이 발생하는 단점이 있다[15].

상황(Context) 중심의 접근제어는 유선 환경에서 무선 환경으로 변화하면서 시간과 장소의 제약을 받지 않는 모델이다[16]. 상황 중심의 접근제어는 시간과 장소의 제한을 받지 않는 서비스를 제공하는 장점은 있지만 자원사이에 역할 계층을 제공하여 사용자에게 적절한 권한을 부여해야 하는 단점이 있다.

III. 사용자 프라이버시를 보장하는 유헬스케어 서비스 모델 설계

유헬스케어 환경에서는 환자의 개인정보에 접근하기 위해 보통 PDAs(Personal Digital Assistants)나 휴대용 컴퓨터를 사용한다. PDAs나 휴대용 컴퓨터는 환자와 더 원활한 통신을 할 수 있고 환자 개인정보를 언제, 어디서든 최신의 갱신된 개인정보에 접근할 수 있도록 도와주지만 제3자에 의한 환자의 개인정보 위험성 또한 많은 문제점이 있다. 이 절에서는 유헬스케어 환경에서 사용자가 사용하는 ID를 통합 관리하여 병원간 환자의 개인정보를 요청할 경우

권한에 따라 환자의 개인 정보를 안전하게 접근할 수 있는 유헬스케어 서비스 모델을 제안한다. 제안된 모델은 실 환경에서 효과적으로 활용할 수 있도록 사용자 신분확인, 병원 권한확인, 진료기록 접근제어, 환자진단 등의 기능으로 구성된다.

3.1. 사용자 통합 ID 관리 모델

환자의 통합 ID를 이용하여 환자의 프라이버시를 보호하기 위한 제안 모델은 [그림 3]과 같다. 제안 모델에서 제공되는 서비스는 원격(화상)진료 서비스, U-방문 간호 서비스, U-자가 서비스 등이 있으며 이러한 서비스를 통해 병원은 환자의 생체정보를 측정하여 환자를 관리한다. 제안 모델에서는 병원의 역할 및 권한에 따라 사용자의 데이터베이스 접근을 제어하며 사용자의 ID를 서버에서 통합 관리한다.

환자의 프라이버시 위협이 증가되는 환경에서 병원이나 약국에서 환자의 기록을 이용할 경우에 제안 모델에서는 병원이나 약국에게 제한된 권한을 부여하여 환자의 동의에 따라 진찰 및 치료 내역을 이용할 수 있도록 하여 환자의 의료정보를 안전하게 보호하고 있다.

[그림 3]의 제안 모델에서는 사용자의 권한확인 및 기록 접근제어 등을 통하여 환자, 병원, 약국의 권한을 분리하여 최소한의 업무를 줌으로써 허가받지 않는 제 3자가 쉽게 환자의 민감한 의료정보 및 개인정보에 접근하지 못하도록 하여 환자의 프라이버시를 보장하고 있다. 기존 유헬스케어 서비스 모델에서는 병원마다 서로 다른 환자 식별 체계가 사용되고 있어 환자는 다양한 형태, 다수의 ID 정보를 기억 및 관리해야 하는 문제점을 가지고 있다. 그러나, 제안 모델은 병원간 건강/의료 정보 공유 시, 환자를 포함한 인가 받은 정보 소비 주체들이 불필요한 개인 정보 노출 없이 익명성을 보장 받으면서 정상적인 인증 및 식별이 가능하도록 사용자 통합 ID 관리 정보를 관리함으로써 환자 인증 및 관리 효율성을 향상시키고 있다.

특히, 환자 인증 및 관리 효율성 측면에서 제안 모델은 중대형 병원내의 서버간 사용자의 건강 정보 요청 및 접근이 수행됨으로써 사용자 건강 정보 요청자의 식별, 접근 제어, 교환 데이터의 기밀성과 무결성 보장, 발생하는 정보 이벤트에 대한 보안 감사 등을 지원하며 접근제어를 위한 RBAC이나 PMAC 등의 정의를 접근 제어 정책에 추가하여 안전한 사용자 건강 정보를 서버간 공유한다.

또한, [그림 3]에서 환자 자신이 아닌 사용자가 병원이나 약국의 데이터베이스에 저장되어 있는 환자의 진료 기록을 이용할 경우 제한된 권한을 사용자에게 부여하는 동시에 환자의 동의에 따라 진찰 및 치료 내역의 이용 범위를 제한하게 된다. 이 같은 과정은 병원이 환자의 처방전을 약국에 전송할 때 환자진료기록의 데이터베이스에 환자 정보를 추가한 후 사용자 정보 데이터베이스와 정보를 동기화하는 동시에 사용자 현황 및 기본진료기록 데이터베이스에 정보를 업데이트함으로써 불법적인 환자 데이터베이스 조작을 예방하여 환자의 프라이버시를 보장하고 있다.

3.1.1 구성요소

제안 모델을 구성하는 구성요소는 [그림 4]처럼 생체 및 환경 정보를 센싱, 모니터링 하기 위한 의료 센서나 기기, 센서 간 통신 및 데이터 송·수신을 위한 유·무선 네트워크, 생체데이터 분석과 건강 피드백을 담당하는 의료 정보 서버, 그리고 생성된 의료 정보를 소비하는 다양한 정보 소비자 집단, 즉 환자나 의료진 및 관련 응용 서비스, 사용자 정보를 저장 및 관리하는 데이터베이스 등으로 구성된다.

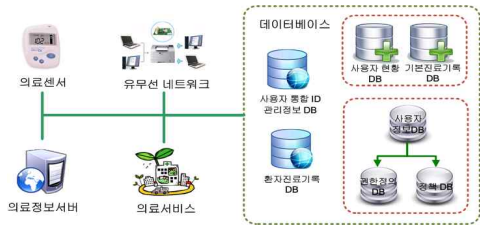


그림 4. 제안 모델의 구성요소
Fig. 4. Component of proposed model

[그림 4]에서 사용되는 데이터베이스는 사용자 ID를 통합 관리하는 사용자 통합 ID 관리정보 데이터베이스, 사용자 현황 정보를 관리하는 사용자 현황 데이터베이스, 환자의 진료기록을 저장하는 기본진료기록 데이터베이스, 사용자 정보에 접근하는 사용자의 권한 및 접근 정보를 담당하는 사용자 정보 데이터베이스 등이 있으며, 사용자 정보 데이터베이스는 권한 정의 데이터베이스와 정책 데이터베이스로 구성된다

3.1.2 주요기능

제안 모델에서 사용되는 환자 인식형 혹은 이동형 센서는 환자의 식별 정보를 포함하여 혈당, 당뇨, 심박 수, 동작 탐지 등에 관한 생체 정보를 측정하고 필요에 따라 주변 환경 정보 등을 감지하여 동기식 혹은 비동기식적인 방법으로 유·무선 네트워크를 통해 건강 정보 서버에 전송한다. 이 때, 무선 의료 기기 및 센서 간에는 Zigbee 나 UWB 방식의 센서 통신 프로토콜이 사용될 수 있으며 WLAN이나 3GPP, 이더넷 등을 포함한 유무선 인터넷을 통해 수집된

데이터들이 전송된다.

의료 정보 서버는 전송된 정보의 ID를 통합 관리함으로써 병원간 환자의 정보를 공유할 경우 환자 정보에 접근할 수 있는 권한을 부여하여 데이터베이스에 저장되어 있는 환자의 정보를 동기화한다. 건강 정보 시스템에 수집 및 축적된 데이터로부터 건강상태, 생활패턴 등에 관한 건강 자료를 분석하고 이와 관련된 경고, 현장진단 처방, 단순 주지 등의 피드백이 응용서비스의 한 형태로 사용자에게 전송된다.

3.2. 분산 처리기법을 이용한 사용자 신분 확인 및 인증

[그림 5]에서 분산처리기법을 이용한 사용자 신분 확인 및 인증과정은 사용자 신분이 병원(의사, 간호사), 약사, 환자, 미가입자 등으로 분류되어 사용자가 명확한지 검증한 후 일반 텍스트 파일 형태로 저장된 환자의 기본 속성을 비밀분산 기법을 이용하여 인증하는 과정이다[11].

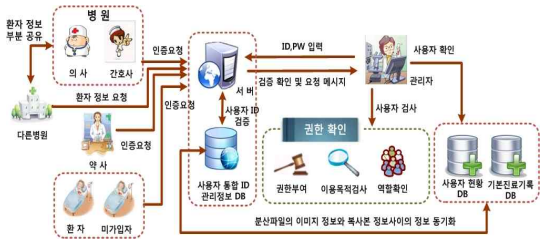


그림 5. 분산처리기법을 이용한 사용자 신분 확인 및 인증
Fig. 5. User Verification and Authentication using Distribution Process

[그림 5]에서 일반 텍스트 파일 형태로 서버에 분산 저장된 민감한 개인정보는 관리 미숙으로 인한 개인정보의 오·남용 및 유출공격 등을 통한 환자의 신용정보 또는 의료정보와 같은 민감한 정보가 일부 유추된다하더라도 제안 모델에서는 개인정보를 부분 변형 또는 암호 저장되기 때문에 제3자가 개인저보를 복구할 수 없게 한다. 특히, 제안 모델은 분산파일 시스템의 일부 서버가 정지되거나 통신을 할 수 없는 상황이라도 저장된 데이터 중 threshold 값 이상의 일부만을 사용하여 복구를 보장하고 있다.

[그림 5]에서 환자의 프라이버시를 보장하기 위한 분산파일 시스템 구조는 분산 파일의 이미지 정보를 갖고 있는 서버와 파일 복사본을 갖고 있는 서버로 구분하여 환자의 프라이버시 정보를 사용자의 이미지 테이블이 있는 사용자 통합 ID 관리 정보 데이터베이스와 사용자 정보 데이터베이스가 있는 서버에 각각 나누어 저장한다. 이 같은 방법은 대규모의 파일조작을 지원하고 여러 개의 파일 복사본을 관리함으로써 가용성을 보장할 수 있다.

환자의 개인정보가 분산 저장되면 인증서를 통해 신분 확인 후 개인 정보 보호 정책에 준한 환자의 속성을 분산 처리할 수 있도록 PKI를 활용한다. 이는 사용자의 접근 권한, 임무, 역할 등의 속성 정보만을 따로 관리하는 속성 인증서를 생성하고 관리하여 시스템이 신원 확인 후, 신원에 따라 주어진 그룹에 할당하고 이 후 설정된 정책등급과 속성정보를 가지고 권한을 부여하여 정책 기반의 접근제어가 이루어지도록 한다. 환자가 요청할 경우에는 사용자 신분검사를 통해 신분을 확인함으로써 사용자는 자신의 개인정보(신분, 재산 및 병력)와 진료 및 처방 기록을 모두 볼 수 있다.

3.2.1 환자 정보 분산저장

제안 모델에서 환자의 개인정보를 분산저장하기 위한 방법으로 환자의 개인정보를 병원(의사, 간호사), 타병원, 약사, 환자, 미가입자 등의 개인정보 $M_l=\{M_l|M_l\in M,\ 1\le l\le L\}$로 추출하여 $m_l=C(M_l)$로 변환한다. 여기서 L은 분산된 개인 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.

서버에서 임의의 소수 $q(q\ge n+1)$를 선택한 후 Z_q에서 $a_i(1\le i<t)$을 선택한 후 이진수로 변환된 개인정보 k를 상수항으로 하는 임의의 $t-1$차 다항식 $f(x)=k_l+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1}(\mathrm{mod}\ q)$를 선택한다. 서버는 조각난 개인정보를 $S_j=f(x_j)$로 계산하여 의사 또는 간호사에게 n개의 $S_j(1\le j\le n, t\le n)$를 비밀 분산하여 저장한다.

3.2.2 환자 정보 복구 및 조회

최소 t이상의 개인정보에 대해서 S_j를 수집한다. 수집된 정보는 서버에서 보관하고 있는 $f(x)$의 계수 a_i와 x_j을 이용하여 라그랑지 보간법(Lagrange Interpolation)으로 $f(0)=k_l$을 복원하거나 행렬식으로 해를 구하는 방법을 사용한다. 라그랑지 보간법으로 복원된 조각난 개인정보 k_l는 모든 l에 대해서 반복적으로 $M_l=C^{-1}(k_l)$ 형태로 변환 작업을 수행한 후 M_l을 $M=M_1\cup M_2\cup\cdots\cup M_L$으로 만들어 환자의 개인정보를 복구 및 조회한다.

3.3. 권한확인 및 제어

제안 모델에서는 병원(약사,간호사), 타병원, 약사, 환자, 미가입자 등으로 제안 모델에 접속하는 사용자를 분류하고

분류된 사용자의 역할에 따라 제한된 권한을 부여한다. 이때, 사용자에게 부여되는 권한은 역할기반의 접근제어(Role Based Access Control)을 사용하며 제안모델에서는 권한을 사용자에게 직접 부여하는 것이 아니라 제안 모델에서 필요로 하는 역할을 의료 업무에 따라 분류하여 권한을 부여한다. 제안 모델은 사용자의 역할에 따라 개인정보 데이터를 접근할 수 있는 제한적인 권한을 부여하고, 개인정보 요청 목적과 조건에 따라 접근을 제한하기 때문에 시스템을 이용하는 사용자에게 할당되는 업무나 기능을 편리하게 추가 및 삭제할 수 있다.

제안 모델은 사용자의 역할을 구분하여 의료 업무에 따라 권한을 할당받고 할당된 범위내에서 업무 및 기능을 수행한다. 병원 간 의료 정보 전달의 상호 호환성을 위해서 환자는 병원을 방문하고 서버에 등록된 통합 ID을 이용하여 병원에서 기다리는 시간/비용을 절감하면서 보다 편리하고 체계적인 의료서비스를 이용할 수 있다. [표 1]은 제안 모델에서 권한 확인 및 제어를 위해 역할기반의 접근제어에서 사용되는 구성요소들이며 각 구성요소의 역할을 정의하고 있다.

환자의 기록에 접근하는 의사는 병원 인증을 통해 역할 및 권한을 확인한다. 병원이 환자의 진단 기록을 요청했을 때 병원의 권한을 검증하고 정보 이용목적을 확인하여 정의된 의료정보정책과 일치한다면 환자기록에 접근 가능하도록 한다. 유헬스케어 환경에서 제안 모델은 병원의 신분 확인을 통해 병원 간의 임무분리와 최소권한을 주어 환자의 개인 정보 유출 및 진료 정보의 손실을 예방하고, 권한 없는 자의 정보 접근을 제어하기 위한 기능을 제공한다

표 1. 구성요소
Table 1. Component

요소	설 명
사용자	USHS 모델을 이용하는 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
제약 사항	사용자가역할에 할당되는 조건, 역할 내 의료 업무의 제한조건, 정보의 이용에 필요한 제약조건 등

3.4. 환자 진료기록 접근제어

환자의 생체정보를 관리하기 위해서 의사는 환자의 진찰 기록이 저장되어 있는 기본진료기록 데이터베이스에 접근할 때, 환자의 프라이버시 보호를 위해 의사는 환자의 병명 및 진료 기록만을 보고 환자의 개인정보는 낮은 레벨의 정보만을 본다.

만약 환자가 다른 병원에서 진찰한 진료 기록이 있거나 보안 등급이 높은 특이 질병이 있을 경우에 병원은 다른 병원에 환자의 상세진료 기록내용을 요청하고 사용자에게 진료기록 접근 여부를 Notice 기능으로 요청하여 사용자의 전 진료기록을 본다. 이때, 병원은 환자의 진료기록을 다른 병원에 전달하기 전에 환자의 부분 ID 정보를 병원에 전달하여 병원이 소유하고 있는 환자의 부분 ID 정보와 함께 사용자 통합 ID 관리정보 데이터베이스에 환자의 ID가 일치하는지 검증한다. 이 같은 과정을 통해 환자는 자신의 개인정보를 병원이 불법적으로 남용하지 않도록 할 수 있다. 또한, 병원(의사, 간호사, 약사)에 보안등급의 정책을 설정하여 의료업무별 역할을 구분하여 병원과 약국, 사용자에게 임무분리 및 최소한의 권한만을 주어 환자의 진료기록에 대한 보안등급별 접근제어를 수행하여 개인 정보 유출 및 진료 정보의 손실을 예방한다.

의사는 환자의 진단내용이나 병명에 접근하려고 할 때 환자의 진찰내용에 대한 권한이 확인된 후 보안 등급 정책설정에 따라 등급별로 기록이 가능하다. 만일 환자의 진찰내용이 합법적인 의사에 의해서 추가된다면 환자의 진료기록은 환자 진료기록 데이터베이스와 기본진료기록 데이터베이스에 각각 업데이트된다. 진료가 끝난 사용자의 처방내용은 합법적으로 등록된 약국에게 전송되고 약국은 자신의 역할에 따라 제한된 권한만 부여되어 사용자의 처방약에 대해서만 접근한다.

IV. 평가

이 절에서는 유헬스케어 서비스에서 발생할 수 있는 가장 대표적인 공격유형으로 제안기법의 안전성을 평가하고 사용자 수에 따른 인증 서버의 처리시간과 오버헤드 등으로 효율성을 평가한다.

4.1 실험환경

이 절에서는 인증서버의 인증 처리시간과 오버헤드를 평가하기 위한 도구로 OPNET을 사용하였다. 실험을 위하여

(표 1)의 실험 시나리오를 사용한다. 실험에서 설정된 사용자 수는 100, 500, 1,000, 1,500, 2,000명이며 인증 서버의 최대 수는 3으로 설정한다. 실험 시간은 86,400초 동안 실험을 수행한다. 사용자 기기의 버퍼 크기는 100패킷의 크기를 가지는 것으로 가정하며, 각 패킷은 패킷 전송동안 패킷 드롭 확률을 0.01로 한다. 이 같은 설정은 현실 모델에 맞는 시뮬레이션을 만들기 위한 설정들이다.

표 2. 실험 환경
Table 2. Experiment Environment

환경 변수	값
사용자 수	100, 500, 1,000, 1,500, 2,000
인증서버의 최대수	3
실험시간	86,400 s
버퍼 크기	100 packet/s
패킷 드롭 확률	0.01
데이터 패킷 크기	100 bytes
쿼리 패킷 크기	25 bytes
헤더 패킷 크기	25 bytes

[표 2]의 실험 환경은 제안 모델과 기존 모델을 동일한 환경에서 실험하기 위한 설정값으로써 기타 설정값은 반영하지 않고 실험하는 것으로 가정한다.

4.2. 효율성 평가

4.2.1 사용자 수와 암호 알고리즘에 따른 인증서버의 인증 처리시간

[그림 6]은 유헬스케어 인증서버와 사용자 사이에 송·수신 되는 인증 정보에 암호 알고리즘 HMAC(SHA-1),RIPEMD-256, AES/ECB(256-bit key) 그리고 RC5을 EAP-AKA 인증 유형에 적용한 사용자의 인증 처리 시간을 평가하고 있다. 실험 결과 사용자 수 증가에 따른 인증서버의 인증 처리시간은 비례적으로 증가하였으며, 가입자 수가 1,000명 이하일 경우에는 인증 처리시간의 증가율이 일정하게 증가하였지만 가입자 수가 1,000명 이상일 경우에는 인증서버의 오버헤드로 인해 인증 처리시간의 증가율이 급격하게 증가하였다.

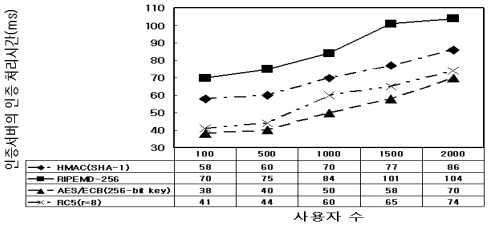


그림 6. 사용자 수와 암호알고리즘에 따른 인증 서버의 인증 처리시간
Fig. 6. Authentication Process Time of Authentication Server through User Number and Encryption Algorithm

표 3. 실험 환경
Table 3. Experiment Environment

단위 : ms

모델명 / 사용자수	제안모델				P-RBAC 모델				목적기반 접근제어모델				상황중심접근모델			
	HMAC (SHA-1)	RIPEMD-256	AES/ECB (256-bit key)	RC5 (r=8)	HMAC (SHA-1)	RIPEMD-256	AES/ECB (256-bit key)	RC5 (r=8)	HMAC (SHA-1)	RIPEMD-256	AES/ECB (256-bit key)	RC5 (r=8)	HMAC (SHA-1)	RIPEMD-256	AES/ECB (256-bit key)	RC5 (r=8)
100	58	70	38	41	74	79	55	63	66	76	51	59	65	73	41	46
500	60	75	40	44	82	86	62	69	69	84	55	62	67	79	45	50
1000	70	84	50	60	88	93	74	76	75	90	60	68	72	88	53	63
1500	77	101	58	65	94	109	76	80	84	106	65	73	80	104	62	70
2000	86	104	70	74	99	112	80	87	89	109	75	79	88	106	72	76

표 4. 실험 환경
Table 4. Experiment Environment

모델 / 인증 서버수 / 사용자수	제안모델			P-RBAC 모델			목적기반 접근제어모델			상황중심접근모델		
	1	2	3	1	2	3	1	2	3	1	2	3
100	0.1	0.05	0.03	0.3	0.17	0.08	0.24	0.13	0.07	0.15	0.08	0.05
500	0.25	0.17	0.1	0.45	0.37	0.21	0.31	0.25	0.18	0.27	0.2	0.14
1000	0.4	0.37	0.33	0.53	0.46	0.4	0.46	0.4	0.37	0.44	0.38	0.35
1500	0.53	0.42	0.4	0.6	0.55	0.51	0.55	0.51	0.47	0.54	0.49	0.43
2000	0.6	0.55	0.52	0.83	0.75	0.64	0.75	0.64	0.6	0.71	0.65	0.55

[그림 7]은 제안모델, P-RBAC 모델, 목적기반 접근모델, 상황중심접근모델 등에 인증 정보의 암호알고리즘을 적용하여 비교 평가한 결과이다. 기존 모델과 제안 모델의 평가 결과는 [표 3]와 같으며, 실험 결과 사용자 정보를 최소하여 인증서버의 인증 권한 정보를 습득한 제안모델이 기존 모델에 비해 인증처리 시간이 10.8% 향상되었다.

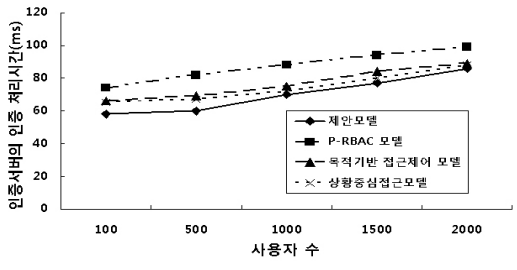
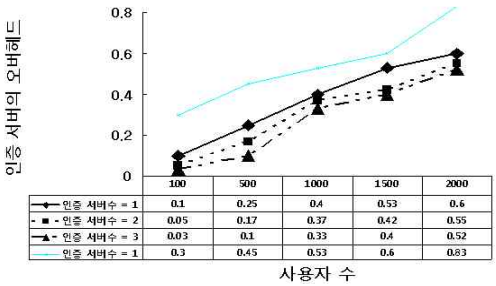


그림 7. 인증 서버의 인증 처리시간 비교
Fig. 7. Compare of User Number and Encryption Algorithm

4.2.2 사용자 수에 따른 인증서버의 오버헤드

[그림 8]은 사용자 수에 따른 인증 서버의 오버헤드를 비교 평가하고 있다. [그림 8]에서 인증서버의 수는 유헬스케어 서비스 확장에 따라 관리자가 인증서버를 1에서 3까지 그룹 관리되는 것으로 실험하였다.



	100	500	1000	1500	2000
인증 서버수 = 1	0.1	0.25	0.4	0.53	0.6
인증 서버수 = 2	0.05	0.17	0.37	0.42	0.55
인증 서버수 = 3	0.03	0.1	0.33	0.4	0.52
인증 서버수 = 1	0.3	0.45	0.53	0.6	0.83

그림 8. 사용자 수에 따른 인증서버의 오버헤드
Fig. 8. Overhead of Authentication Server through User Number

실험 결과 사용자 수가 증가함에 따라 인증 서버의 오버헤드는 점진적으로 증가하였으며, 500~ 1,000명 사이에서 인증서버의 수와 상관없이 모두 인증서버의 오버헤드가 급격하게 증가하였다. 그러나 [그림 8]의 결과를 기반으로 인증서버 당 사용자수를 그룹 관리할 경우 그룹 관리하지 않을 경우보다 인증서버의 오버헤드는 최대 25%까지 줄일 수 있었다.

[그림 9]는 제안모델, P-RBAC 모델, 목적기반 접근모델, 상황중심접근모델 등의 인증서버의 오버헤드를 비교 평가한 결과이며, 기존 모델과 제안 모델의 인증서버의 오버헤드 평가 결과는 [표 4]와 같다. 실험 결과 제안 모델이 기존 모델보다 평균 8%가 인증 서버의 오버헤드가 낮게 나타났다.

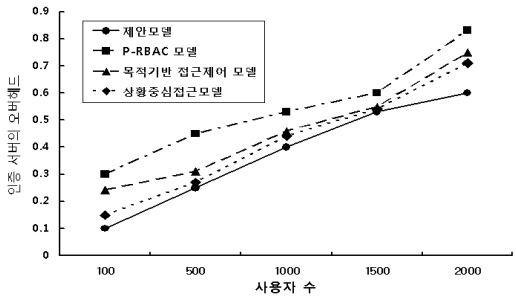


그림 9. 인증서버의 오버헤드 비교
Fig. 9. Compare of Overhead of Authentication Server

4.3. 보안평가

4.3.1 내부공격

① 다단계 서비스 접근인증에 따른 공격

유헬스케어 서비스 및 기기 접근을 위한 방법으로는 외부 서비스 사업자를 통한 CP 서비스 접근인증, 사업자 인증 서버 접근을 위한 네트워크 사업자 제공 유헬스케어 서비스 접근 인증 및 원격접근 인증, 지역 인증 서버를 통한 원격 접근 인증, 홈 및 병원 내 게이트웨이나 서버에 보안 기능을 탑재한 각기 접근 인증 방법 등이 있다. 제안 모델에서는 인증 서버에 접근하기 위해서는 접근권한에 따른 다단계 서비스 접근인증을 통해 서비스를 허용하는 방법을 사용하기 때문에 권한이 없는 사용자가 사용자의 정보를 불법적으로 접근하지 못한다. 특히, 제안 모델에서는 유헬스케어 디바이스 및 서버가 접근 권한에 따라 상호간 등록 및 인증 요청, 키 교환, 디바이스 인증 정보 전송, 인증 결과 전송 등이 완료된 후에만 서비스가 정상적으로 제공된다. 사용자 인증 메커니즘 또한 디바이스 인증과 동일한 방법으로 서비스 요청이 발생할 경우 서버 인증서전송, 인증 키 교환 과정 등을 수행 후에만 서비스를 정상적으로 이용할 수 있다.

② 서비스 거부 공격

제안 모델이 서비스 거부 공격에 대응 하는 방안으로는 서버에 접근하는 사용자에 대해서 접근 제어에 대한 우선순위를 지정하도록 하여 서버에 접근하는 사용자를 손쉽게 관리하도록 하고 있다. 그리고, 불법 접근 공격을 방어하기 위해서 기밀성을 제공하는 암호화 기법을 사용하여 유헬스케

어 서비스를 위해 사용되는 모든 기기의 인증 체계를 강화하는 방법을 사용하고 있다.

③ 사용자 프라이버시 공격

제안 모델에서 환자의 프라이버시를 보장하기 위해서 시스템을 분산 파일 시스템 구조를 갖도록 하였다. 제안 모델의 분산 파일 시스템 구조는 분산 파일의 이미지 정보를 갖고 있는 서버와 파일 복사본을 갖고 있는 서버로 구분하여 환자의 프라이버시 정보를 사용자의 이미지 테이블이 있는 사용자 통합 ID 관리 정보 데이터베이스와 사용자 정보 데이터베이스가 있는 서버에 각각 나누어 저장한다. 이 같은 방법은 대규모의 파일조작을 지원하고 여러 개의 파일 복사본을 관리함으로써 가용성을 보장할 수 있어 사용자의 프라이버시를 보호할 수 있다.

4.3.2 외부공격

① 전송되는 과정에서의 정보 공격에 따른 보안

유헬스케어 환경에서 병원(의사)은 무선통신용 AP 또는 공유기를 통해 전달되는 환자의 생체 정보의 변화를 모니터하고 요구사항에 따라 정보를 서버내에 사용자 데이터베이스에 저장하는 역할을 수행한다. 그러나 환자의 생체정보 수집 및 전송 범위가유헬스케어 환경에서는 제한적이기 때문에 악의적인 사용자가 있을 경우 서버로 전달중인 사용자 정보를 공결할 수 있다. 기존에 단-대-단 통신을 하는 메커니즘에서는 악의적인 사용자를 추출하기 위해서 수집된 정보내에 MAC을 포함하도록 하여 데이터를 판독하지만 일정 기간 동안 악의적인 사용자가 올바른 판독작업을 방해하기 때문에 문제가 발생할 수 있다. 제안 기법에서는 이 같은 문제를 해결하기 위해서 단-대-단 방식 대신 홉-대-홉 방식을 사용하여 환자를 인증하기 때문에 서버가 환자의 정보를 판독하는 동안 악의적인 사용자가 판독작업을 방해하지 못하도록 한다. 이것은 모든 키를 서버가 집중 관리하지 않고 사용자 정보를 분산 관리하는 중간 역할을 하는 서버에게 키 관리 역할을 분배하였기 때문에 가능하다. 그리고 서버가 정보를 수집한 후 통신 범위내에 침입 노드를 인식하면 수신되는 모든 메시지 전송을 중지함으로써 침입자 공격을 예방할 수 있다.

② Blackhole/Sinkhole 공격에 따른 보안

Blackhole/Sinkhole 공격에서는 악의적인 사용자가 유헬스케어 서비스의 모든 트래픽을 끌어들이기 위해서 blackhole처럼 동작한다. 특히 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. 제안기법에서는 t 시간 간격으로 서버가 생성한 그룹키 K를 유헬스케어 서비스를 제공받는 환자들과 환자의 정보를 담당하는 서버에게 전달하여 이전에 사용한 그룹키 K를 갱신하기 때문이다. 이 때, 계층적으로 구성된 중간역할을 하는 서버가 pair-wise 키를 사용하여 환자 정보와 키 정보를 암호화한 후 홉-대-홉 방식으로 CRC(Cyclic Redundancy Check)을 전송함으로써 서버는 암호화된 데이터 값만을 수집하게 된다.

③ Hello 플로우 공격에 따른 보안

유헬스케어 서비스에서 Hello 플로우 공격은 높은 주파수 전송 범위와 프로세스 파워를 가지는 악의있는 공격자가 유헬스케어 서비스가 제공되는 전 지역에 분산된 환자들에게 HELLO 패킷을 보냄으로써 악의있는 공격자를 병원(의사, 간호사)으로 인식하여 스푸프(spoof)하게 한다. Hello 플로우 공격을 예방하기 위해서 제안기법에서는 키 분배 과정 중 이동하는 패킷을 버퍼에 저장한다. 환자는 이전의 키로 패킷을 복호화하고, 새로 생성된 키로 암호화하여 패킷을 전송하게 된다. 제안된 기법은 키 분배 중 이동하는 패킷의 보안을 위해 아래와 같은 보안 특성을 가지고 수행한다.

- 데이터 비밀 유지: 강력한 대칭 키 암호 기법 알고리즘과 공개키 암호 기법 알고리즘을 혼용하여 유헬스케어 서비스를 제공받는 환자간 안전한 통신을 보장한다.
- 데이터 인증: 사용자 정보와 함께 암호화된 서명은 인증을 보장하는 소스 ID를 지닌다. 제안 기법은 브로드캐스트 통신 인증을 제공하지 않는다. 이 방법은 암호 기호 알고리즘 키의 주기적 변경에 의존한다.
- 데이터 무결성: 서명 내의 CRC는 메시지가 수정되지 않도록 보장한다. 서명은 암호화돼 있으므로 데이터 무결성을 보장한다.
- 데이터 최신성: 세션과 서명 내의 계수기 모두 약한 데이터 최신성에 기여한다. 병원은 세션과 착신되는 패킷의 서명 내의 계수기를 기대한다. 이 세션이 현재 세션보다 높은 경우, 약한 신선도가 확보된다. 반면에 이 세션이 현재 세션과 동일하면 계수기를 확인하게 된다. 서명 내의 더 큰 계수기 값은 약한 데이터 신선도를 보장하여 서비스 거부(DoS: denial of service) 공격을 방지한다.

④ 웜홀 공격에 따른 보안

웜홀(Wormhole) 공격은 공격자가 네트워크의 특정 위치에서 패킷(또는 비트)을 기록하고 다른 위치에 있는 환자와 직접 터널을 맺는 위험한 공격방법이다. 패킷의 터널링이

나 재전송 방법은 선택적으로 수행되지만 웜홀 공격은 무선 센서 네트워크에서 매우 위협적이다. 그 이유는 공격자가 네트워크내 환자들과 타협을 요구하지 않거나 서버가 환자 정보를 복구하기 시작할 때 초기 구문에서 수행될 수 있기 때문이다. 제안 기법에서는 웜홀 공격을 예방하기 위해서 신규 환자가 유헬스케어 서비스에 합류하려고 할 때 신뢰성 있는 비밀 키 K_m를 가지고 있도록 한다. 이 신규 환자는 합류하고자 하는 유헬스케어 서비스 내에 있는 서버에게 요청 메세지를 전송한다. 전송 후에 서버는 임의의 수(nonce)를 신규 환자에게 전송한다. 환자는 단방향 기능을 이용해 P'를 $P' = F(nonce, P)$로 계산한다. 유헬스케어 서비스를 제공받는 환자들은 공통의 숫자 P'를 지니게 된다. 신규 환자는 키를 획득함으로써 유헬스케어 서비스에 포함된다.

- 환자의 병원 서비스내 이동: 제안 기법은 환자의 병원 서비스내 이동을 지원한다. 병원 서비스내의 환자들은 공통 키 K_m를 지니고 있기 때문에 병원 서비스 내에서 자유롭게 이동이 가능하다. 따라서 병원 서비스를 제공받는 환경에서 환자 이동은 추가 보안 작업이 필요하지 않다.
- 환자의 병원간 이동: 제안 기법은 환자의 병원간 이동을 지원한다. 환자는 병원 H_i을 떠나면서 병원 H_i의 키를 삭제하게 된다. 또한 환자가 병원 H_j에 합류하기 위해서는 병원 H_j의 키를 필요로 한다. 이런 경우는 병원에 합류하는 신규 환자와 동일한다. 신규 환자에 신뢰성 있는 비밀 키 K_m이 있는 경우 제안 기법은 환자의 합류를 지원한다.

⑤ Sybil 공격에 따른 보안

Sybil 공격은 무선 네트워크에서 임무를 수행하는 여러 환자들의 정보를 합병하기 위해서 합법적인 인식자를 사용하여 위장하는 공격 방법이다. Sybil 공격은 분산된 저장공간, 라우팅 메커니즘, 데이터 수집, voting, 공정한 자원 할당과 오용 탐지등에서 발생될 수 있다. 제안 기법에서는 Sybil 공격을 예방하기 위해서 2개 이상의 병원에 포함되는 공통 환자를 지원한다. 공통 환자는 공통 환자들이 속하는 모든 병원의 키를 보유한다. 이웃 병원에서는 일정 시간 간격을 두고 키 변경이 발생할 수 있다. 패킷을 병원 H_i에서 병원 H_j로 전송하기 전에 환자는 우선 병원 H_j의 키로 패킷을 암호화하고, 그 후에 H_j의 키로 복호하게 된다. 이 같은 과정을 홉-대-홉 방식으로 진행해 나감으로써 Sybil 공격을 예방하게 된다.

V. 결론

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 유헬스케어 환경에서 사용자의 프라이버시를 보호하기 위해서 환자의 ID 정보를 사용자 상태 및 접근 레벨에 따라 통합/분할 관리할 수 있는 유헬스케어 서비스 모델을 제안하였다. 제안된 모델은 실 환경에서 효과적으로 활용할 수 있도록 사용자 신분확인, 병원 권한확인, 진료기록 접근제어, 환자진단 등의 기능으로 구분하였다. 또한, 사용자의 ID가 중앙의 서버에서 통합 관리되는 동시에 병원간 공유되는 사용자의 정보에 대한 프라이버시를 보호하기 위해서 사용자의 보안 레벨 및 권한에 따라 사용자의 ID를 병원에 분할 적용하여 제 3자에 의한 사용자의 프라이버시 침해 및 의료정보 유출을 예방하였다.

보안 평가에서는 헬스케어 서비스에서 발생할 수 있는 가장 대표적인 공격유형으로 제안기법의 안전성을 평가한 결과, 기존 모델에서 제기되었던 다양한 보안 문제점이 개선된 결과를 얻을 수 있었다. 향후 연구에서는 병원(의사, 약사, 직원)과 환자 사이에 안전한 ID를 통합관리를 위해 사용되는 키를 효율적으로 관리할 수 있는 키 관리 프로토콜을 평가 할 예정이다.

참 고 문 헌

[1] T. M. Song, S. H, Jang, “u-Healthcare : Issue and Research Trends“, Korea Institute for Health and Social Affairs, pp. 119-129, Jan. 2011.

[2] K. J. Kim, S. P. Hong, “Privacy Information Prot ection Model in e-Healthcare Environment”, Korean Society for Internet Information, Vol. 10, N., 2, pp. 29-40, Apr. 2009.

[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] E. Y. Kim, M. Lee, "Multi-agent-based U-healthcare system for Managing Hypertension", International Conference on convergence Information Technology, pp. 1694-1699, Nov. 2007.

[12] Crypto++ 5.6.0 Benchmarks, http://www.cryptopp.com/benchmarks.html

[13] Q. Ni, A. Trombetta, E. Bertino and J. Lobo, "Privacy-aware Role Based Access Control", The Proceedings of the 12th ACM Symposium on Access Control Models and Technologies, pp. 41-50, Jun. 2007.

[14] Q. Ni, D. Lin, E. Bertino and J. Lobo, "Conditional Privacy-aware Role Based Access Control", The Proceedings of the 12th European Symposium on Research in Computer Security, LNCS 4734, pp. 72-89, 2007.

[15] J. W. Byun, E. Bertino and N. Li, "Purpose based access control of complex data for privacy protection", Proceedings of the tenth ACM symposium on Access control models and technologies (SACMAT'05), pp. 102-110. Jun. 2005.

[16] N. Gustaf, S. Mark, "An Approach to Engineer and Enforce Context Constraints in an RBAC Environment", Symposium on Access Control Models and Technologies(SACMAT 2003), pp. 65-79, Jun. 2003.

저 자 소 개

이 봉 근

1982년 : 숭실대학교 전자계산학과 학사

1985년 : 숭실대학교 산업대학원 전자계산학과 석사

2000년 : 충북대학교 대학원 전자계산학과 박사수료

1986년~현재 : 부산경상대학 소방안전계열 교수

관심분야 : 네트워크 보안, 정보보안

Email : rbk@bsks.ac.kr

정 윤 수

2000년 : 충북대학교 대학원 전자계산학 이학석사

2008년 : 충북대학교 대학원 전자계산학 박사

2009년~현재 : 한남대학교 산업기술연구소 전임연구원

관심분야 : 센서 보안, 암호이론, 정보보호, 이동통신보안

Email : bukmunro@gmail.com

이 상 호

1976년 : 숭실대학교 전자계산학과 학사

1981년 : 숭실대학교 전자계산학과 석사

1989년 : 숭실대학교 전자계산학과 박사

1981년~현재 : 충북대학교 소프트웨어학과 교수

관심분야 : 네트워크보안, Protocol Engineering, Network Management

Email : shlee@cbnu.ac.kr