상태정보에 따른 체내삽입형 장치를 부착한 유-헬스케어 환자의 프라이버시 보호 프로토콜

정회원 정 윤 수*°, 이 상 호**

U-Healthcare user's privacy protection protocol with Implantable medical Device of State Information

Yoon-Su Jeong*°, Sang-Ho Lee** *Regular Members*

요 약

최근 유헬스케어 시스템은 IT 기술과 의료서비스가 접목되면서 사용 범위가 점점 넓어지고 있다. 그러나 유헬스케어 시스템 중 체내삽입형 장치를 사용하는 환자의 경우, 환자의 프라이버시 예방과 안전한 접근 제어에 대한 대비책이 마련되어 있지 않아 그에 따른 프라이버시 보호 문제가 대두되고 있다. 본 논문에서는 체내삽입형 장치를 사용한 환자의 프라이버시를 보장하기 위해서 환자 정보를 가상화한 후 환자의 상태값과 수행값을 동기화함으로써 제3자의 불법적 접근을 예방할 수 있는 환자 프라이버시 보호 프로토콜을 제안한다. 제안된 프라이버시 보호 프로토콜은 사전에 관리 서버에 등록된 병원(의사, 간호사, 약국 등)의 권한정보에 따라 체내삽입형 장치를 부착한 환자의 개인정보의 열람범위를 제한하여 병원관계자의 불법적 업무 수행을 예방한다. 특히, 체내삽입형 장치와 게이트웨이 역할을 하는 가상장치는 접근 허가가 승인된 환자 정보 이외에 허가받지 않은 정보에 대해서 제 3자가 쉽게 접근하지 못하도록 환자의 상태값과 수행값을 동기화함으로써 환자의 프라이버시 관리의 효율성을 향상시키고 있다.

Key Words : u-헬스케어(u-Healthcare), 프라이버시(Privacy), 접근제어(Access Control)

ABSTRACT

IT technology of U-healthcare system is being grafted onto medical services and the use of U-healthcare system are extending steadily. However, in case of patients using Implantable Medical Device (IMD) in U-healthcare system, patients' privacy protection and safe access to system recently has emerged as a major issue. This paper proposes a patients' privacy protection protocol to prevent any illegal accesses from third parties as state value and action value are synchronized after patients' information virtualization. The proposed protocol can limit the access range of patients' information according to authentication information of hospitals, doctors, nurses, and pharmacies registered in the U-healthcare server. Additionally, this protocol can increase management efficiency for patients' privacy by synchronizing state values and action values only for approved information and, by instituting this process, third parties cannot easily access patients' information.

Ⅰ. 서 론

최근 의료 서비스 분야에서 각광을 받고 있는 유헬스케어(u-Healthcare) 서비스는 유·무선 네트워킹과 전자 의료기기를 통해 언제, 어디서나 이용 가능한 건강관리 및 의료 서비스를 지원하면서 환자의

* 목원대학교 정보통신공학과 교수(bukmunro@mokwon.ac.kr), (° : 교신저자)
** 충북대학교 소프트웨어학과 교수(shlee@chungbuk.ac.kr)
논문번호 : KICS2012-02-062, 접수일자 : 2012년 2월 20일, 최종논문접수일자 : 2012년 3월 20일

질병에 대한 원격관리와 일반인의 건강 유지 및 향상을 목적으로 한다[1,2]. 유헬스케어 서비스는 기존 의료서비스에 유비쿼터스 기술을 접목하여 언제, 어디서나, 보건의료 서비스를 제공하고자 바이오정보를 포함한 개인정보와 의료정보를 다루기 때문에 해킹으로 인한 정보유출 사고발생시 국가적인 혼란과 사회적인 불신을 야기할 수 있다[3].

특히, 유헬스케어 시스템 중 체내삽입형 장치(IMD, Implantable medical Device)는 일반적으로 불치병을 치료하기 위해 사용되며 환자의 생명과 개인 정보가 직접적으로 연관되어 있기 때문에 접근제어와 프라이버시 예방이 매우 중요하다. 만일 체내삽입형 장치가 접근제어를 제공하지 않거나 의사에게 승인된 사람만이 접근한다면 환자를 위험에 빠지게 할 수 있다.

체내삽입형 장치의 보안요구사항은 D. Halperin et al.[4]에서 제시하였으며, D. Halperin et al.[5]은 체내삽입형 장치에 악의적인 접근이 발견될 경우 알람이 울리는 기법을 제안했다. 비록 공격을 탐지하고 나중에 측정되더라도 이 기법은 근본적인 공격에 대한 예방은 제공되지 않고 있다.

C. Israel et al.[6]은 근거리에서만 체내삽입형 장치에 접근하는 기법을 제안했다. 이 기법은 메시지의 통신시간을 측정하고 특정 시간이 초과할 경우 액세스를 거부하는 방법을 사용한다. 그러나 이 방법은 전화통신이 가능한 장비를 사용하여 원거리에서 공격자가 체내삽입형 장치에 접근할 수 있는 문제점이 있다[7]. 이 문제를 해결하기 위해서 Kasper B. Rasmussen et al.[8]은 전달된 소리 신호의 차이를 검증하는 기법을 제안했다. 그러나 이 기법은 공격자가 장치 설정을 통해 퍼미션을 얻어 액세스를 시도할 수 있는 문제점을 가지고 있다. Tamara Denning et al[9]은 [8]을 개선하기 위해서 은폐장치를 사용한 체내삽입형 장치 시스템을 제안했다. 이 기법에서 사용되는 은폐장치는 외부에서 제어할 수 있는 외부장치로써 공격자가 손쉽게 접근하여 환자의 생체정보를 얻을 수 있는 문제가 있다.

본 논문에서는 체내삽입형 장치를 사용한 환자의 프라이버시를 보장하기 위해서 환자 정보를 가상화한 후 환자의 상태값과 수행값을 동기화함으로써 제3자의 불법적 접근을 예방하는 환자 프라이버시 보호 프로토콜을 제안한다. 제안된 프로토콜은 사전에 관리 서버에 등록된 병원(의사, 간호사, 약국 등)의 권한정보에 따라 체내삽입형 장치를 부착한 환자의 개인정보의 열람범위를 제한하여 병원이 최소한의 업무를 수행하도록 한다. 특히, 체내삽입형 환자와 게이트웨이 역할하는 가상장치는 접근 허가가 승인된 환자 정보 이외에 허가받지 않은 정보에 대해서 제 3자가 쉽게 접근하지 못하도록 환자의 상태값과 수행값에 따라 접근을 허용하도록 함으로써 환자의 프라이버시 관리의 효율성을 향상시키고 있다.

이 논문의 구성은 다음과 같다. 2장에서는 유헬스케어 서비스 개념과 체내삽입형 장치를 사용한 유헬스케어 시스템에 대해서 알아본다. 3장에서는 체내삽입형 장치를 부착한 환자이 프라이버시를 보호하는 프로토콜을 제안하고, 4장에서는 제안 프로토콜의 안전성과 효율성을 평가하고, 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련연구

2.1. 유헬스케어 서비스

유헬스케어 서비스는 IT 기술을 의료기술에 접목하면서 환자의 상태정보를 언제, 어디서나 수집, 처리, 전달, 관리 할 수 있게 함으로써 환자의 건강 및 의료서비스를 제공하는 서비스이다[5]. 유헬스케어 서비스는 기존 의료 서비스를 지원하면서 서비스의 편리성을 높이기 위해 유·무선 온라인 네트워크를 활용한 전자적 의료정보 및 진료 예약관리 등을 진화시킨 서비스이다.

유헬스케어 서비스는 센싱, 모니터링, 분석 및 피드백 등의 3가지 단계로 동작한다[1,2]. 센싱 과정은 인체에서 발생하는 물리적·화학적인 현상의 변화를 감지하여 처리 가능한 전기적 신호로 변환하는 기능을 수행한다. 모니터링 과정은 측정된 생체정보를 의미 있는 생체신호 성분만을 선택하기 위한 필터링 처리와 의미 있는 정보로 만들기 위한 분석과정, 그리고 이를 시각화하기 위한 기능을 수행이다. 분석 과정은 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 정보나 생활 변화를 사용자의 행동변화, 경고 등으로 사용자에게 제공하는 과정이다.

2.2. 체내삽입형 장치를 사용하는 유헬스케어 시스템

체내삽입형 장치는 환자의 생명정보(호흡, 심장

박동수, 온도, 혈합 등)를 수집하기 위해서 환자 몸에 삽입한 장치를 말한다. 제세동기(또는 잔떨림 제거기), 심장병환자 박동 조율기 등과 같은 체내삽입형 장치는 원거리에 있는 환자를 진찰할 수 있다. 따라서 체내삽입형 장치는 심장질환, 당뇨병 등과 같은 불치병을 위한 해결책을 제공한다. 의사는 환자의 상태를 실시간으로 체크하고 체내삽입형 장치는 환자 자신의 몸을 쉽게 관리할 수 있다. 미국에서는 약 25만명의 환자가 체내삽입장치를 가지고 의학 서비스를 제공받고 있다. 유헬스케어어 시스템은 환자가 언제, 어디서나 의사에게 환자 자신의 상태를 보내 서비스를 제공받는다. 유헬스케어 시스템은 체내삽입형 장치와 함께 환자의 상태를 24시간 모니터하여 문제가 발생할 경우 바로 탐지한다.

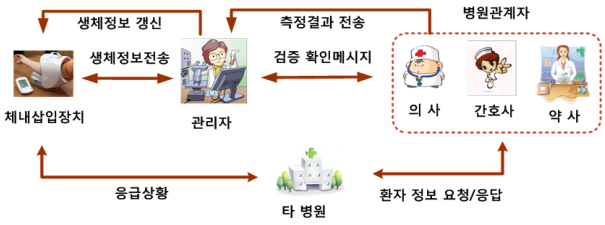

그림 1. 유헬스케어 시스템의 구조
Fig. 1. Structure of u-Healthcare System

그림 1은 체내삽입형 장치를 가지는 환자가 유헬스케어 시스템에서 동작하는 구조를 보여주고 있다[9]. 체내삽입형 장치를 구성하는 유헬스케어 시스템은 체내삽입형 장치, 관리자, 병원관계자, 서버 등으로 구성된다. 병원관계자는 체내삽입형 장치로부터 환자의 생체 정보를 체크하기 위해서 관리자에게 환자의 생체 정보를 요청한다. 환자는 자신의 상태 정보를 수시로 체크하기 위해서 관리자가 제공하는 서비스를 제공받는다.

Ⅲ. 체내삽입형 장치를 부착한 환자의 프라이버시 보호 프로토콜

이 절에서는 유헬스케어 서비스를 제공받는 체내삽입형 장치를 부착한 환자의 상태값과 수행값을 동기화시켜 환자의 프라이버시를 보호하는 프로토콜을 제안한다. 제안 프로토콜은 병원관계자의 권한에 따라 관리자가 환자의 정보 열람을 제한하며 불법적인 접근시도가 발생할 경우 환자의 상태값과 관리자의 수행값을 비교 검증함으로써 서비스 제공여부를 판별한다.

3.1. 개요

체내삽입장치를 부착한 환자의 프라이버시를 보장하기 위한 제안 프로토콜의 구조는 그림 2와 같다.

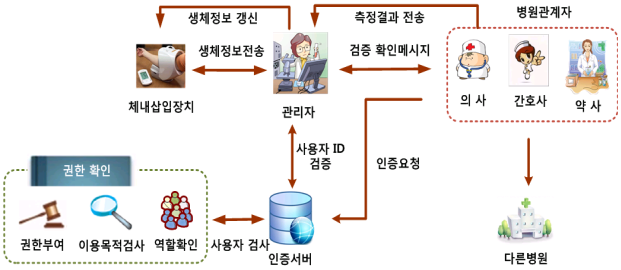

그림 2. 제안 프로토콜의 구조
Fig. 2. Structure of Proposed Protocol

제안 프로토콜은 병원 관계자에게 특정 권한을 부여하여 권한에 따라 환자 정보 열람을 제한하도록 접근 제어와 인증을 수행한다. 체내삽입 장치내 환자 정보를 제3자가 불법적으로 접근하는 것을 예방하기 위해서 관리자는 환자를 가상화하여 환정 정보에 접근하는 병원관계자의 접근을 제어하고 인증을 수행한다. 환자에게 접근하는 병원관계자의 접근을 제어하는 방법으로는 체내삽입장치와 관리자가 사전에 동의한 상황값(상태값과 행위값 등)의 동기화로 병원 관계자가 환자의 정보를 요청할 경우 사전 등록된 정보와 비교 검증을 통해 수행된다.

3.2. 구성요소

그림 2처럼 제안 프로토콜은 체내삽입장치, 관리자(=Cloaker), 병원관계자, 인증서버 등으로 구성된다. 체내삽입장치는 환자에 부착되며, 환자의 생체정보를 측정하고 프로그램된 펌웨어에 따라 동작된다. 체내삽입장치는 제약된 전력과 계산적 비용이 낮은 장치를 사용하며 5미터 범위 내에서 통신이 가능하다. 병원관계자는 체내삽입장치의 환자 생체정보를 수집하는 역할을 수행하며 체내삽입장치에게 환자의 갱신된 생체정보를 보내는 역할을 수행한다. 관리자는 체내삽입장치와 병원관계자의 중계자 역할을 하며 유·무선 통신이 가능하다. 관리자는 체내삽입장치와 달리 높은 계산능력과 수용능력이 있으며 다양한 정보(키, 로그 데이터 등)을 저장할 수 있는 역할을 수행한다. 인증서버는 병원관계자가 체내삽입장치에 접근하기 위해서 인증서버에 사전에 저장된 정보와 비교분석을 통해 권환을 부여받아 체내삽입 장치를 부착한 환자의 생체정보의 열람 권한 레벨을 부여하는 역할을 수행한다.

3.3. 용어정의

제안 프로토콜에서 사용하는 주요 용어를 정의하면 표 1과 같다.

3.4. 프로토콜

이 절에서는 체내삽입 장치를 부착한 환자의 프라이버시를 보장하기 위해서 체내삽입 장치의 환자 정보를 합법적으로 접근하기 위한 프로토콜로써 정보 등록과정, 프라이버시 보장을 위한 인증과정 과정 등의 2단계로 구성된다.

3.4.1. 정보 등록과정

등록과정은 병원관계자가 체내삽입 장치를 부착한 환자의 생체정보를 요청하기 전에 환자 정보와 병원관계자의 권한 정보를 사전에 인증 서버에 등록하는 과정으로써 등록 과정은 그림 3과 같이 5단계로 구성된다.

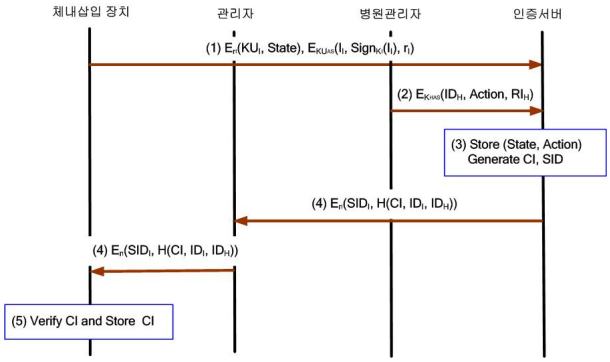

그림 3. 등록과정
Fig. 3. Registration Process

• 단계 1 : 환자는 체내삽입 장치에 대해서 유헬스케어 서비스를 제공받기 전에 인증 서버에 사용자 정보를 전달하는 단계로써 환자는 인증 서버에게 환자의 인식자 $KU_I(=ID_I)$와 패스워드 $KR_I(=KU_I \bullet g^{r_I})$를 해쉬 함수 $H(\bullet)$에 적용하여 환자 정보 $I_I=H(KU_I,\ KR_I)$를 생성한다. 생성된 환자 정보는 환자의 패스워드로 서명한 후 랜덤수 r_I와 함께 암호화하고 환자의 상태값 $State$은 환자의 개인키 KU_I로 암호화하여 식 (1)처럼 인증 서버에게 전달하여 등록한다. 여기에서 상태값 $State$는 0과 1의 값에 따라 정보의 갱신 유·무가 판별된다.

$$E_{r_I}(KU_I,\ State),\ E_{KU_{AS}}(I_I,\ Sign_{KR_I}(I_I),\ r_I) \tag{1}$$

표 1. 용어 정의
Table 1. Terminology Definition

용 어	정 의
I,M,H,AS	각각의 개체(I: 체내삽입장치, M : 관리자, H : 병원관계자, AS : 인증서버)
K_{IM}	체내삽입장치와 관리자 사이의 공유키
K_{MH}	관리자와 병원관계자 사이의 공유키
K_{MAS}	관리자와 인증서버 사이의 공유키
K_{HAS}	병원관계자와 인증서버사이의 공유키
ID_X	X의 아이디
SID_X	X의 보안 인식자
PU_X/PR_X	X 의 공개키/개인키
KU_X/KR_X	X 의 ID기반 공개키/개인키
State	체내삽입장치의 상태값
Action	관리자의 수행값
r_X	x가 생성한 랜덤수
$Sign_K(m)$	개인키 K로 메시지 m을 서명
I_X	X의 정보
RI_X	X의 권한정보
sk	인증서버가 생성한 비밀키
$\|$	연접(concatenation)
$\oplus$	exclusive-OR
$H()$	512비트 이상의 출력을 갖는 암호학적으로 안전한 해쉬 함수
$HMAC()$	해쉬 MAC 함수
SID	보안 인식자
$E_X[m]$	키 X로 메시지 m을 암호화

• 단계 2 : 병원관계자는 인식자 ID_H와 수행값 $Action$, 권한정보 RI_H 등을 인증서버와 공유된 키 K_{HAS}로 암호화하여 인증서버의 데이터베이스에 전달하여 저장한다. 여기서 실행값 $Action$은 상태값 $State$과 동일하게 0과 1의 비트 값에 따라 정보의 갱신 유·무가 판별된다.

$$E_{K_{HAS}}(ID_H,\ Action,\ RI_H) \tag{2}$$

• 단계 3 : 인증서버는 환자로부터 전달받은 상태값 $State$와 병원관계자로부터 전달받은 실행값 $Action$을 병원관계자와 인증서버 사이의 공유키 K_{HAS}로 복호화하여 쌍으로 묶은 후 데이터베이스에 저장한다. 인증서버는 체내삽입 장치 정보 I_I와 병원관계자의 접근 권한 정보 RI_H를 관리자와 인증서버 사이의 공유키 K_{MAS}로 $HMAC(\bullet)$에 적용한 후 인증서버

의 정보 I_{AS}와 exclusive-OR 하여 연계 정보 CI로 대체한다.

$$CI = HMAC_{SK}((I_I \,||\, RI_H) \oplus I_{AS}) \quad (3)$$

• 단계 4 : 인증서버는 생성한 CI를 환자의 인식자 ID_I, 병원관계자의 인식자 ID_H와 함께 해쉬 함수 $H(\bullet)$에 적용한다. 적용된 값은 보안 인식자 SID_U $(=I_I \oplus ID_I)$와 함께 사용자가 생성한 임의의 랜덤수 r_I로 암호화하여 관리자에게 전달한다.

$$E_{r_I}(SID_I,\ H(CI,\ ID_I,\ ID_H)) \quad (4)$$

• 단계 5 : 체내삽입 장치는 관리자로부터 전달받은 정보를 복호화하여 CI 정보를 확인 한 후 체내삽입 장치내 메모리에 저장한다.

$$Verify \text{ CI and } Store \text{ CI} \quad (5)$$

3.4.2. 환자 프라이버시 보장을 위한 인증 과정

이 절에서는 체내삽입 장치를 부착한 환자의 프라이버시를 보장하기 위한 인증 과정으로써 환자가 보유하고 있는 생체 정보를 병원관리자의 권한 레벨에 따라 열람하고 체내삽입 장치의 생체 정보를 갱신하는 과정을 수행한다.

• 단계 1~2 : 병원관계자는 난수 r_H를 생성하여 병원관계자의 인식자 ID_H와 연접하여 관리자와 병원관계자가 공유한 공유키 K_{MH}로 암호화한 후 관리자에게 전달한다.

$$\text{Generate } r_H \quad (1)$$

$$E_{K_{MH}}(ID_H \,||\, r_H) \quad (2)$$

• 단계 3 : 관리자는 공유키 K_{MH}을 이용하여 병원관계자로부터 전달받은 정보를 복호화한 후 관리자 데이터베이스에 저장되어 있는 병원관계자의 인식자 ID_H를 검증한다.

$$\text{Verify } ID_H \quad (3)$$

• 단계 4 : 관리자 데이터베이스에 병원관계자의 인식자 ID_H가 존재하는지 체크하고 만약 존재하지 않는다면 서비스를 종료한다. 관리자는 병원관계자의 인식자 ID_H에 대한 권한 등급 및 레벨에 대한 정보를 검증하기 위해 인증 서버에게 병원관계자의 인식자 ID_H 정보 검토에 대한 의뢰를 요청한다.

$$ID_M\ ,\ E_{K_{MAS}}(ID_M,\ ID_H) \quad (4)$$

• 단계 5 : 인증서버는 관리자로부터 요청된 병원관계자의 인식자 ID_H를 데이터베이스로부터 검색한 후 병원관계자의 인식자 ID_H와 일치하는 정보가 발견될 경우 해당 인식자 ID_H의 퍼미션 정보 $Permission$를 체크한다.

$$\text{Check } ID_H \text{ and Permission} \quad (5)$$

• 단계 6 : 인증서버는 병원관계자의 퍼미션 $Permission$과 권한 정보 RI_H를 추출한 후 체내삽입 장치와 관리자의 상태값 $State$, 실행값 $Action$을 식 (6)처럼 암호화하여 관리자에게 전달한다. 이 때, 인증서버는 체내삽입장치와 동기화를 이루기 위해 체내삽입장치가 인증서버에 등록한 랜덤 수 r_I을 이용하여 ID_I와 I_I 정보를 연접한 결과를 서명한다.

$$ID_M,\ E_{K_{MAS}}(ID_H||Permission||RI_H),\ E_{KU_M}(ID_I,\ State,\ Action,\ Sign_{r_I}(ID_I||I_I)) \quad (6)$$

• 단계 7 : 관리자는 인증서버로부터 전달받은 정보를 K_{HAS}키를 이용하여 복호화한 후 병원관계자의 퍼미션 $Permission$과 권한정보 RI_H를 체크한다.

$$\text{Check } Permission \text{ and } RI_H \quad (7)$$

• 단계 8 : 관리자는 병원관계자의 퍼미션 $Permission$과 권한정보 RI_H를 근거로 체내삽입장치에게 생체정보를 요청한다. 이 때, 체내삽입장치와 관리자의 동기화를 만들기 위해서 관리자의 실행값 $Action$과 체내삽입장치의 상태값 $State$을 인식자 ID_M와 ID_I로 각각 연접하여 보안인식자 SID_I와 함께 공유키 K_{IM}로 암호화한다.

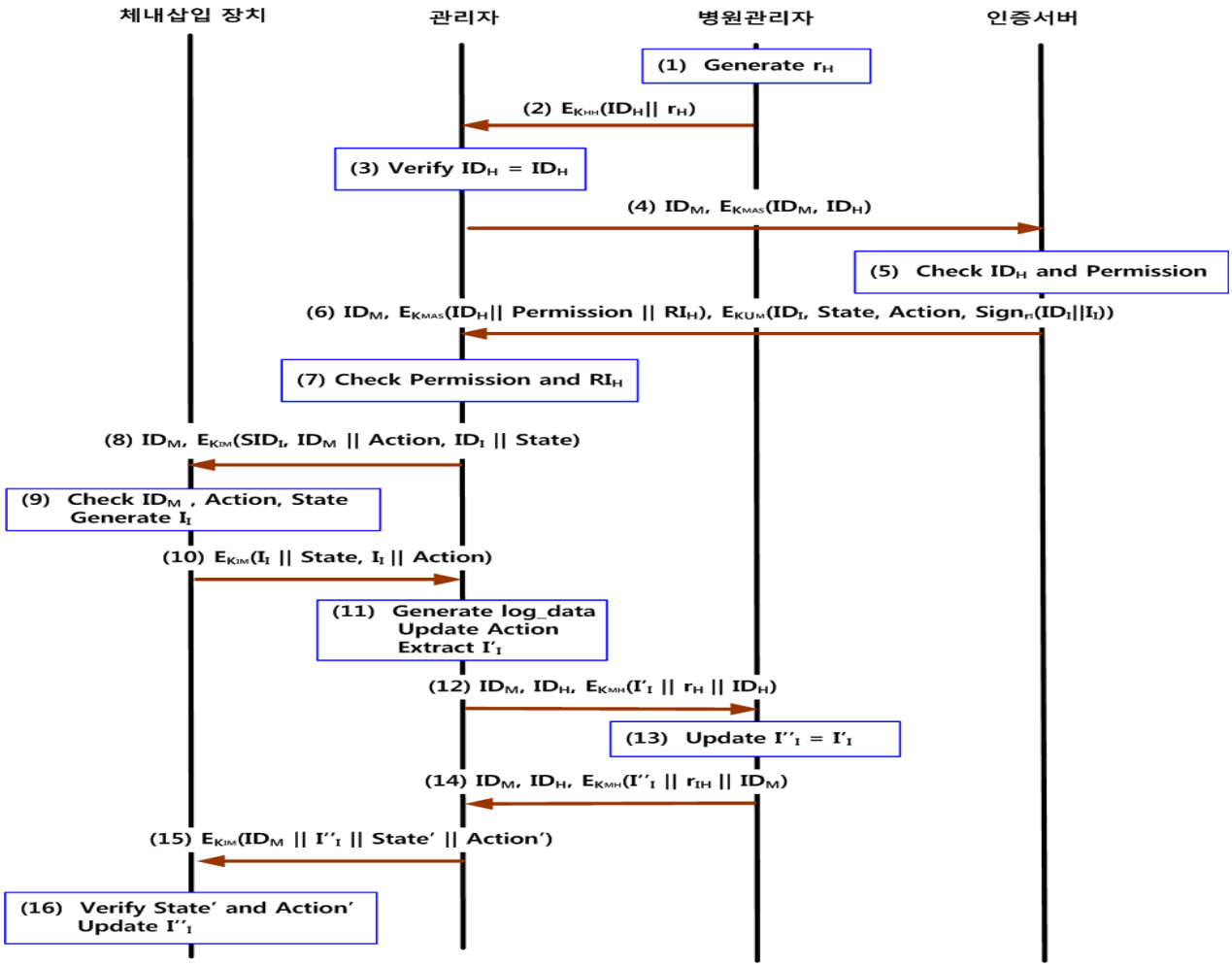

그림 4. 프라이버시 보장을 위한 인증과정
Fig. 4. Authentication Process for Privacy Guarantee

$$ID_M,\ E_{K_{IM}}(SID_I,\ ID_M||\text{Action},\ ID_I||\text{State}) \tag{8}$$

• 단계 9 : 체내삽입장치는 관리자로부터 전달받은 정보를 복호화한 후 ID_M, $Action$, $State$을 체크하고 체내삽입장치에 의해 생성된 생체정보 I_I을 추출한다.

$$\text{Check } ID_M,\ Action,\ State \text{ and generate } I_I \tag{9}$$

• 단계 10 : 체내삽입장치는 추출된 생체정보 I_I를 상태값 $State$과 실행값 $Action$으로 각각 연접하여 관리자에게 공유키 K_{IM}로 암호화하여 전달한다.

$$E_{K_{IM}}(I_I\ ||State,\ I_I\ ||\ Action) \tag{10}$$

• 단계 11 : 관리자는 체내삽입장치로부터 전달받은 생체정보 I_I에 대한 로그 데이터를 생성하고 실행값 $Action$을 갱신한다. 관리자는 병원관계자가 요청한 생체정보 I'_I만을 추출한다.

$$\text{Generate log\_data and Update Action and } Extract\ I'_I \tag{11}$$

• 단계 12 : 관리자는 병원관계자에게 추출된 체내삽입장치의 생체정보 I_I를 병원관계자에게 전달한다.

$$ID_M,\ ID_H,\ E_{K_{MH}}(I_I' \ ||\ r_H \ ||\ ID_H) \quad (12)$$

• 단계 13 : 병원관계자는 관리자로부터 전달받은 체내삽입장치의 생체정보 I_I'를 복호화한 후 새로 진찰된 체내삽입장치의 생체정보 I_I''로 갱신한다.

$$Update\ \ I_I'' = I_I' \quad (13)$$

• 단계 14 : 병원관계자는 체내삽입장치의 생체정보 I_I'를 갱신한 후 관리자로부터 전달받은 갱신된 생체 정보 I_I''와 함께 관리자에게 전달한다. 이 같은 동작은 관리자와 병원관계자 사이의 데이터 동기화를 유지하여 제3자로부터 데이터 안전성을 보장받는다.

$$ID_M,\ ID_H,\ E_{K_{MH}}(I_I'' \ ||\ r_{IH} \ ||\ ID_H) \quad (14)$$

• 단계 15 : 관리자는 병원관계자로부터 전달받은 정보를 추출한 후 병원관계자의 r_H의 무결성을 체크한 후 이상이 없으면 갱신된 생체정보 I_I''을 체내삽입장체에게 전달한다.

$$E_{K_{IM}}(ID_M \ ||\ I_I'' \ ||\ State' \ ||\ Action') \quad (15)$$

• 단계 16 : 체내삽입장치는 관리자로부터 전달받은 정보를 추출하여 상태값 $State'$과 실행값 $Action'$을 검토한 후 생체정보 I_I''을 갱신한다.

$$Verify\ \ State',\ Action' \text{ and } Update\ \ I_I'' \quad (16)$$

Ⅳ. 평 가

이 절에서는 체내삽입형 장치를 사용한 환자의 프라이버시를 보장하는 제안 프로토콜의 안전성과 효율성을 평가한다.

4.1. 보안평가

4.1.1. 권한(Authorizatiojn)

관리자는 기밀 통신을 수행하고 상위 의학 기관의 서명을 검증한다. 관리자와 병원관계자는 오프라인에서 등록하며 등록하지 않은 병원관계자는 관리자와 체내삽입장치에 액세스할 수 없다. 비권한 사람들은 환자와 관련된 정보를 얻을 수 없다. 제안 프로토콜에서는 관리자가 환자의 생체정보를 액세스 퍼미션에 따라 추출하여야만 환자의 생체정보를 얻을 수 있다.

4.1.2. 이용성(Availability)

관리자가 병원관계자와 통신을 중재하고 체내삽입장치와 인식자를 숨김으로써 체내삽입장치에 DoS 공격에 의한 배터리 소비를 예방할 수 있다. 제안 프로토콜에서는 체내삽입 장치를 부착한 환자가 체내삽입 장치의 배터리 상태를 별도로 안전하게 인식할 수 있기 때문에 체내삽입장치의 배터리 교체 시간을 쉽게 알 수 있다.

4.1.3. 장치 설정(Device Setting)

제안 프로토콜에서의 병원관계자는 인증 서버에 등록된 키를 이용하여 명령어를 암호화하고 전달하기 때문에 비 권한 레벨의 공격자는 명령어를 전달할 수 없다. 제안 프로토콜에서는 권한에 따라 명령어 및 환자의 생체정보 열람 범위 제한 및 상태값 $State$과 실행값 $Action$의 동기화, 랜덤 수 r_I을 이용한 인증서버와 체내삽입장치 간 동기화를 통해 체내삽입장치의 안전한 접근 통제를 수행한다.

4.1.4. 프라이버시 예방(Privacy Protection)

체내삽입장치를 사용하기전에 환자는 사전에 관리자와 병원관계자의 권한 및 레벨에 따라 환자의 생체정보에 대한 접근 여부를 인증서버에 등록한 후 환자의 SID와 병원관계자의 권한 및 레벨에 따라 체내삽입장치의 접근 유무가 판별되기 때문에 체내삽입장치의 환자 프라이버시는 안전하게 예방할 수 있다. 또한, 사전에 등록된 공유키는 체내삽입장치, 관리자, 병원관계자, 인증서버가 각각 독립적으로 키를 공유하였기 때문에 제3자가 공유된 키를 유추하기는 어렵고 만약 키를 유추하였더라도 독립적으로 서로 공유된 키를 모두 추출하지 못한다. 그리고, 환자의 보안 인식자 SID_U 는 $I_I \oplus ID_I$ 로 생성되어 공격자가 특정 환자를 식별할 수 없어 환자의 프라이버시를 제공한다.

4.1.5. 환자 익명성

체내삽입장치의 정보 I_I와 인식자 ID_I로 생성된 보안 인식자 SID를 인증서버가 관리자에게 전송하면 관리서버는 체내삽입장치와 함께 서로 상태값과 실행값을 체크하고 병원관계자의 권한 정보와 레벨을 통해 체내삽입장치에 접근하기 때문에 공격자가 체내삽입장치의 생체정보를 불법적으로 추출하려고 하더라도 환자 자신이 생성한 SID를 추측할 수 없기 때문에 환

자의 익명성을 제공한다.

4.1.6. 보안 비교평가

표 2는 제안기법과 Halperin 기법, Rasmussen 기법, Denning 기법들과 공격유형에 따른 보안평가를 비교평가하고 있다.

표 2. 보안 비교평가
Table 2. Compare of Security

모델 / 평가항목	Halperin 기법	Denning 기법	Rasmussen 기법	제안기법
다단계 서비스 접근 인증에 따른 공격	○	×	△	△
서비스 거부 공격	×	△	△	△
사용자 프라이버시 공격	△	×	×	○
Blackhole/Sinkhole 공격	×	○	○	○
Hello 플로우 공격	×	○	○	○
웜홀 공격	×	○	○	○
Sybil 공격	×	○	○	○

× : 지원하지 않음 △ : 일부지원 ○ : 지원

4.2. 성능평가

4.2.1. 실험환경

이 절에서는 인증서버의 인증 처리시간과 인증 지연시간, 오버헤드 등을 평가하기 위한 도구로 OPNET을 사용하였다. 표 3의 실험 환경은 제안 기법과 기존 기법을 동일한 환경에서 실험하기 위한 설정값으로써 기타 설정값은 반영하지 않고 실험하는 것으로 가정한다.

표 3에서 실험에서 설정된 사용자 수는 100, 500, 1,000, 1,500, 2,000명이며 인증 서버는 클라우드 환경에서 인증서를 통해 인증하는 것을 고려하여 최대 수를 1~5으로 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 3. 실험 환경
Table 3. Experimental Environment

환경 변수	값
사용자 수	100, 500, 1,000, 1,500, 2,000
인증서버의 최대수	1~5
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

4.2.2. 인증서버의 인증 처리시간

그림 5는 체내삽입장치의 생체정보를 요청하는 병원관계자의 수에 따른 인증서버의 인증처리 시간을 암호 알고리즘 HMAC(SHA-1), RIPEMD-256, AES/ECB(256-bit key) 그리고 RC5에 따라 인증처리시간을 평가하고 있다. 실험 결과 사용자 수 증가에 따른 인증서버의 인증 처리시간은 비례적으로 증가하였으며, 가입자 수가 1,500명 이상일 경우에는 인증서버의 오버헤드로 인해 인증 처리시간의 증가율이 급격하게 증가하였다.

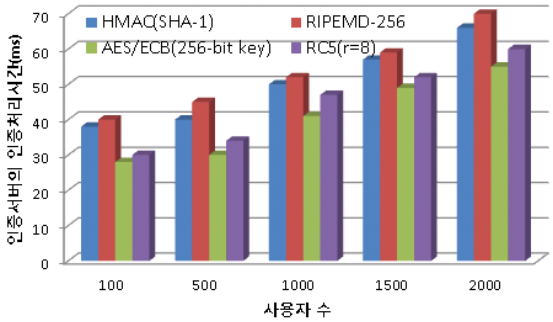

그림 5. 인증 서버의 인증 처리시간
Fig. 5. Authentication Process Time of Authentication Server

4.2.3l 인증서버의 인증 지연시간

그림 6은 사용자 수 증가에 따른 인증 서버의 인증 지연시간을 Halperin 기법, Rasmussen 기법, Denning 기법들과 비교 평가하고 있다. 그림 6에서 사용자 수가 1000명 미만의 경우 Halperin 기법과 제안 기법이 다른 기법에 비해 5.7%와 6.3%만큼 지연 시간이 빠르게 나타났지만 사용자 수가 1000명 이상일 경우 인증 지연시간은 3% 이내로 인증 지연 시간이 큰 차이가 없는 결과를 얻었다.

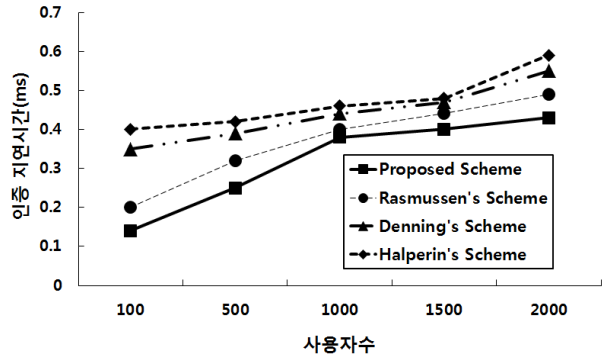

그림 6. 인증 서버의 인증 지연시간
Fig. 6. Authentication Delay Time of Authentication Server

4.2.4. 인증서버의 오버헤드

그림 7은 사용자 수에 따른 인증 서버의 오버헤드를 Halperin's 기법, Rasmussen 기법, Denning 기법들과 비교 평가하고 있다. 그림 7에서 인증서버의 수는 유헬스케어 서비스 확장에 따라 관리자가 인증서버를 1에서 5까지 그룹 관리되는 것으로 실험하였다.

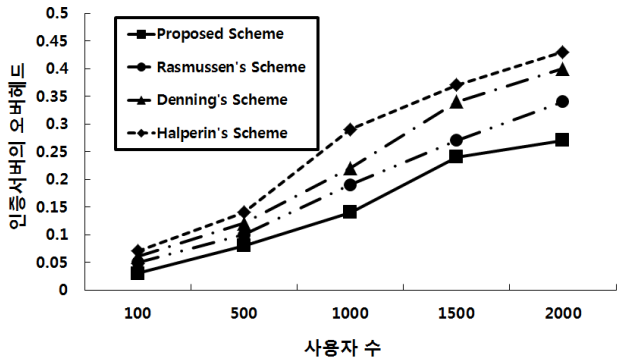

그림 7. 인증 서버의 오버헤드
Fig. 7. Overhead of Authentication Server

그림 7의 실험 결과, 사용자 수 증가에 따라 인증서버의 오버헤드도 비례적으로 증가하는 결과를 얻었다. 그러나, 제안 기법은 환자의 상태값과 수행값을 동기화하는 과정을 수행하여 인증을 수행하기 때문에 제안 기법은 기존 모델보다 인증 서버의 오버헤드가 평균 4.7% 낮게 나타났다.

V. 결 론

최근 유헬스케어에서 서비스가 급증하면서 유헬스케어 서비스를 제공받는 환자의 프라이버시 침해가 증가하고 있는데, 그 중에서, 체내삽입형 장치를 부착한 환자의 프라이버시 침해에 대한 보안 대책이 필요하다. 본 논문에서는 체내삽입형 장치를 사용한 환자의 프라이버시를 보장하기 위해서 환자 정보를 가상화한 후 환자의 상태값과 수행값을 동기화함으로써 제3자의 불법적 접근을 예방하는 환자 프라이버시 보호 프로토콜을 제안했다. 제안된 프로토콜은 사전에 관리서버에 등록된 병원관계자의 권한정보에 따라 업무를 수행할 수 있도록 하여 제3자의 불법적인 정보 유출을 막고 있다. 특히, 체내삽입형 환자와 게이트웨이 역할을 하는 가상장치는 환자의 상태값과 수행값에 따라 접근을 허용하도록 함으로써 환자의 프라이버시 관리의 효율성을 향상시켰다.

향후 연구에서는 제안 프로토콜을 실제 병원 업무에 적용하여 환자의 프라이버시 보호 모델을 구현하고자 한다.

참 고 문 헌

[1] D. W. Kim, J. W. Han, and K. I. Chung, "Trend of Home Device Authentication/Authorization Technology", Weekly IT BRIEF, No. 1329, pp. 1-11, 2008.

[2] S.Y. Lee, K.B. Yim, K.J. Bae, Taeyoung Jeong, and Jong-Wook Han, "Counterplan of Ubiquitous Home Network Privacy based on Device Authentication and Authorization," Korea Institute of Information Security & Cryptology, Review of KIISC, 18(5), pp.125-131, 2008.

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

[4] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemarkers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses", In IEEE Symposium on Security and Privacy. IEEE Computer Society, pp. 1-14, May. 2008.

[5] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, "Security and privacy for implantable medical devices", IEEE Pervasive Computing, Vol. 7, No. 1,

pp. 30-39, Jan. 2008.

[6] C. Israel, s. Barold, "Pacemaker systems as implantable cardiac rhythm monitors", In American Journal of Cardiology, pp. 442-445, Feb. 2001.

[7] I. Kirschenbaum, A. Wool, "How to build a lowcost, extended-range RFID skimmer", Cryptology ePrint Archive: Report 2006/054, 2006.

[8] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based Access Control for Implantable Medical Devices", 16th ACM conference on Computer and communications security, pp. 411-419, Nov. 2009.

[9] T. Denning, K. Fu, and T. Kohno, "Absence makes the heart grow fonder new directions for implantable medical device security", 3rd USENIX Workshop on Hot Topics in Security, pp. 1-7, Oct. 2008.

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~2012년 2월 충북대 및 한남대 시간강사

2012년 3월~현재 목원대학교 정보통신학과 교수

<관심분야> 유·무선 보안, 암호이론, 정보보호, Network Security, 이동통신보안

이 상 호 (Sang-Ho Lee) 정회원

1976년 2월 숭실대학교 전자계산학과 학사

1981년 2월 숭실대학교 전자계산학과 석사

1989년 2월 숭실대학교 전자계산학과 박사

1981년 3월~현재 충북대학교 소프트웨어학과 교수

<관심분야> 네트워크보안, Protocol Engineering Network Management,