연합 ID를 이용한 u-헬스케어 환경의 환자 인증 모델 설계

정윤수*

Design of Patient Authentication Model in u-healthcare Environment using Coalition ID

Yoon-Su Jeong*

요 약 최근 병원에서는 불치병을 갖고 있는 환자에게 의료서비스를 제공하기 위해서 체내에 장치를 부착하여 환자 상태를 모니터링하는 체내삽입장치를 사용하고 있다. 그러나, 유헬스케어 환경을 구성하고 있는 병원관계자가 무분별하게 환자의 생체정보를 악용하여 환자의 생명에 위협을 줄 수 있는 문제점들이 나타나고 있다. 본 논문에서는 병원관계자의 권한레벨에 따라 환자의 생체정보를 사용하기 위한 연합 ID 기반의 인증 모델을 제안한다. 제안 모델은 서로 다른 인증 식별 체계가 사용되고 있는 병원에서 다양한 형태로 존재하는 다수의 ID 정보를 연합하여 병원 간 건강/의료 정보 공유시 불필요한 개인 정보 노출 없이 익명성을 보장받을 수 있다. 특히, 환자 정보에 쉽게 접근할 수 있는 병원관계자의 악의적 행위에 대해서 환자 정보를 안전하게 보호하기 위해서 접근권한에 대한 레벨을 부여함으로써 제 3자가 쉽게 접근하지 못하도록 한다.

주제어 : 체내삽입장치, 인증, 연합 ID

Abstract To provide medical services to patients who have a terminal illness, recent hospital patients to monitor the state of the device attached to the body, the body insertion device is. U-Healthcare Environment and hospital officials indiscriminately exploited by the patient's vital information, however, could threaten the patient's life problems are appearing. In this paper, depending on the level of authority, hospital officials, Union of ID-based authentication model is proposed to use a patient's vital information. Union proposed model identify different authentication system is used in hospitals that exist in various forms in a number of ID information, health / medical information sharing between hospitals without exposure to unnecessary personal information, you can be assured of the anonymity. In particular, with easy access to patient information, hospital officials about the malicious act to protect patient information to access level for the rights granted by third parties to prevent easy access.

Key Words : IMD, Authentication, Federated ID

1. 서론

최근 IT 기술이 생체공학에 적용되면서 체내삽입장치(IMD, Implantable medical Device)를 사용하는 u-헬스케어 서비스가 활성화되고 있다[1]. 체내삽입장치는 일반적으로 인공심장, 전자인식표, 혈액 투속기, 보청기 등 불치병을 치료하기 위해 많이 사용되고 있다. 그러나 체내삽입장치처럼 무선의료기기을 사용하는 장치들은 무선으로 의료 정보를 송신하기 때문에 악의를 가진 제3자가 악용할 수 있어 보안 문제가 발생할 수 있다[2].

현재 체내삽입장치의 데이터를 안전하게 보호하는 방법은 크게 3가지로 분류할 수 있다. 첫째, 체내삽입장치에서 전달되는 정보를 암호화된 상태에서 유지하며, 관리자만이 이를 복호화하는 방법이 있다. 이 방법은 체내

*목원대학교 정보통신공학과 조교수 : 교신저자
논문접수: 2013년 2월 20일, 1차 수정을 거쳐, 심사완료: 2013년 3월 15일, 확정일: 2013년 3월 20일

삽입장치에서 전달되는 데이터가 신뢰적이지 못하다는 가정하에 동작되며, 구현이 어렵다는 단점이 있다. 둘째, u-헬스케어 환경에서 특정 보안영역에서만 접근제어와 암호화 기술을 사용하는 방법이있다. 이 방법은 다양한 보안 기술을 적용할 수 있지만 보안 요구사항을 모두 적용하기 어려운 단점이 있다. 셋째, 단순히 환자에 부착된 체내삽입장치가 보낸 데이터를 신뢰하는 방법이 있다. 그러나, 체내삽입장치에서 보낸 데이터를 이용하여 환자에게 의료 서비스를 제공하는 유-헬스케어 측면에서 보면 이 방법은 데이터의 신뢰도가 낮기 때문에 유-헬스케어 서비스에 적용하기에는 어려운 문제점이 있다.

연합 ID를 사용하는 사용자가 하나의 신뢰영역에 등록한 하나의 ID를 이용하여 자신의 신뢰영역 뿐만 아니라 다른 신뢰영역에서도 인증을 받기 위해서는 단일 신뢰영역이 아닌 다중 신뢰영역간의 ID 연동을 위한 연합 ID가 제공되어야 한다[3,4]. 예를 들어, 체내삽입장치를 사용하는 환자가 갑자기 응급상황이 발생할 경우, T. Denning et. al[5]는 환자의 체내삽입장치의 물리적 환경 속성 값을 이용하여 응급 환자를 치료하는 fail-open 개념을 제안하였다. 그러나, 이 기법은 체내삽입장치의 물리적 환경 변화의 상태 정보를 이용하여 체내삽입장치를 공격하는 공격방법을 탐자할 수 이는 장점은 있지만 공격에 대한 사전 예방은 할 수 없다는 단점이 있다.

본 논문에서는 체내삽입장치를 부착한 환자의 생체정보를 병원관계자(의사, 간호사, 약사 등)가 요청할 경우 병원관계자의 권한레벨에 따라 생체정보를 지역에 관계없이 접근할 수 있도록 연합 ID를 기반으로 인증하는 모델을 제안한다. 제안 모델은 연합 ID 관리 시스템 모델에서 기본적으로 제공하는 안전성, 신뢰성, 프라이버시를 기본적으로 제공하면서 서로 다른 인증 식별 체계가 사용되고 있는 병원에서 다양한 형태로 존재하는 다수의 ID 정보를 연합하여 병원 간 건강/의료 정보 공유시 불필요한 개인 정보 노출 없이 익명성을 보장받도록 인증 정보에 대해서 권한을 제한한다. 특히, 환자 정보에 쉽게 접근할 수 있는 병원관계자의 악의적 행위에 대해서 환자 정보를 안전하게 보호하기 위해서 접근 허가가 승인된 환자 정보 이외에 허가받지 않은 정보에 대해서 제 3자가 쉽게 접근하지 못하도록 한다.

이 논문의 구성은 다음과 같다. 2장에서는 유헬스케어 환경의 체내삽입장치에 대해서 알아본다. 3장에서는 연합 ID 관리 시스템 모델을 제안하고, 4장에서는 유헬스케어 환경에서 발생하기 쉬운 보안 공격유형에 따른 안전성을 평가하고, 마지막으로 5장에서 결론을 맺는다

2. 관련연구

2.1 체내삽입장치

유헬스케어 환경에서 병원관계자(의사, 간호사, 약사 등)는 체내삽입장치를 통해 언제 어디서나 환자의 생체정보를 수집, 전달, 관리 할 수 있다. 여기서 체내삽입장치는 환자의 생명정보(호흡, 심장박동수, 온도, 혈압 등)을 수집하기 위한 생체삽입 장치를 의미한다[5]. 체내삽입장치는 원거리에 있는 환자를 진찰할 수 있기 때문에 심장질환, 당뇨병 등과 같은 불치병을 위한 해결책을 제공하고 있다. 유헬스케어 환경에서 체내삽입 장치를 부착한 환자의 상태(협압, 당뇨, 심전도, 체지방 분석 등)의 정보를 인터넷을 통해 유헬스케어 서비스 센터에게 전달하여 병원관계자(의사)가 환자의 상태정보를 분석한 후 환자의 처방을 피드백한다.

2.2 기존 연구분석

최근 체내삽입장치를 사용하는 환자가 증가하면서 체내삽입장치에 대한 연합 ID 모델에 대한 연구의 필요성 또한 증가하고 있다. Z. A. Khattak et. al[6]는 공격자(adversary)가 체내삽입장치에 접근을 시도할 경우 연합 ID 관리 시스템에서 연합 ID의 공격유형에 따라 안전하게 연합 ID를 관리할 수 있는 보안 모델을 제시하고 있다. Z. A. Khattak et. al는 연합 ID 관리 시스템에 대한 보안 모델을 기반으로 클라이언트와 인식자 제공자 사이의 신뢰적 설립을 위한 상호 플랫폼을 제안하였다. H. Gao et. al[7]은 연합 ID 관리을 위한 동적 신뢰 모델을 제안하였다. 이 모델에서는 동적 신뢰 관계를 정책적으로 표현하기 위해서 동적 신뢰 정책 언어를 통해 신뢰관계를 표현하고 있다.

2.3 연합 ID 관리 시스템

대부분의 연합 ID 관리 시스템 모델은 커버러스(Kerveros), Liberty Alliance, OPENID, Windows Live ID 등이 있다. 커버러스는 도메인간 네트워크 인증 시스템이다. 커버러스 보안 사회기반시설(infrastructure)은 모든 사용자와 서베스 제공자가 프라이버시 위험을 가지

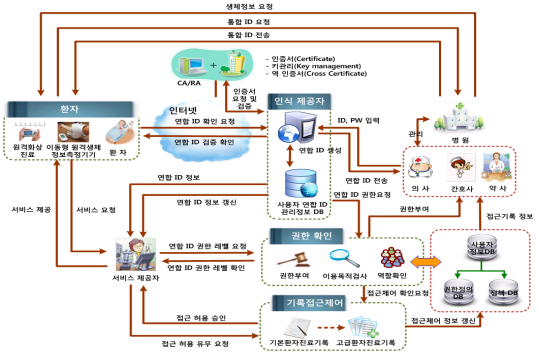
는 암호 동작을 수행하기 위한 인증 서버와 함께 long-term 비밀키을 공유하는 대칭키 암호화에 기반한다. 커버러스는 트로이 목마, man-in-the-middle 공격과 같은 내부공격에 대해서 패스워드에 대한 신뢰된 경로의 요구로 인하여 패스워드 추측에 대해서 효율적이지 못하다. Liverty alliance 은 140개 이상의 회사들이 연합하여 구성된다.

3. 연합 ID 기반 통합 인증 모델

이 절에서는 환자의 생체정보를 언제, 어디서든 접근하기 위한 연합 ID기반 통합 인증 모델을 제안한다. 제안된 모델은 실 환경에서 활용하기 위해서 사용자 인증, 병원 권한관리, 접근제어 등으로 구성된다.

3.1 개요

체내삽입장치의 생체정보를 언제, 어디서나 안전하게 병원관계자(의사/간호사/약사 등)들이 사용할 수 있도록 병원관계자들의 인증을 효율적으로 처리하기 위한 연합 ID 기반의 사용자 인증 모델은 그림 1와 같다.



[그림 1] 연합 ID기반의 사용자 인증 환경

그림 1에서 제안 모델은 병원관계자의 역할 및 권한에 따라 환자의 생체정보의 접근을 제한함으로써 사용자의 프라이버시를 보장하고, 서비스 제공자가 병원관계자의 연합 ID의 권한 레벨에 따라 환자의 생체정보를 병원관계자에게 제공함으로써 생체정보에 대한 신뢰성을 보장한다. 또한 제안 모델에서는 연합 ID를 실제 ID가 아닌 가상의ID로 만들기 위해서 병원관계자의 ID, 패스워드와 같은 정보를 조합하기 때문에 보안성을 제공한다. 또한 제안 모델은 연합 ID를 사용하기 때문에 병원간 건강/의료 정보 공유 시, 병원관계자를 포함한 인가 받은 사용자의 불필요한 개인 정보 노출 없이 사용자의 익명성을 보장 받으면서 정상적인 인증 및 식별이 가능한 사용자 연합 ID를 관리함으로써 병원관계자 인증 및 관리의 효율성을 향상시키고 있다. 특히, 병원관계자 인증 및 관리 효율성 측면에서 기존 기법보다 서버간 사용자의 건강 정보 요청 및 접근이 원활하게 수행될 수 있을뿐만 아니라 사용자 건강 정보 요청자의 식별, 접근 제어, 교환 데이터의 기밀성과 무결성 보장, 발생하는 정보 이벤트에 대한 보안 감사 등을 지원할 수 있다.

그림 1에서 인식 제공자는 병원관계자에게 특정 권한을 부여하여 권한에 따라 환자 정보를 열람할 수 있도록 접근 제어와 인증을 수행한다. 만약 제 3자가 불법적으로 인증을 수행하려고 하거나 체내삽입장치에 접근하려고 할 경우 인식 제공자는 접근을 제어한다.

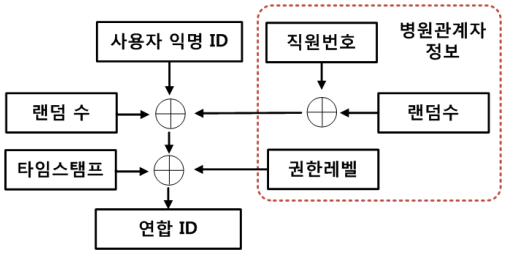
3.2 사용자 신분 인증

체내삽입장치를 부착한 환자의 생체정보를 병원관계자가 요청할 경우 병원관계자는 표 1처럼 사용자의 익명정보, 병원관계자 정보(직원번호, 권한등급, 랜덤값 등) 그리고 타임스탬프 등을 조합하여 병원내에서 사용할 수 있는 연합 ID를 생성하여 사용자의 신분을 인증하는데 사용할 수 있다.

〈표 1〉 연합 ID 생성 항목

사용자 익명 ID	병원관계자			타임스탬프
	직원번호	권한등급	랜덤수	

그림 2은 연합 ID를 생성하기 위한 연합 ID 생성과정을 보여주고 있다. 연합 ID를 생성하기 위해서는 환자가 사용하는 익명의 인식자와 병원관계자의 정보가 조합되어 만들어진다.

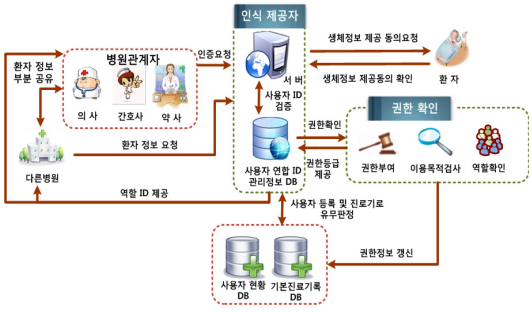


[그림 2] 연합 ID 생성 과정

그림 2에서 연합 ID의 생성은 병원관계자와 환자의 익명 ID를 조합한 후 생성된 병원관계자의 권한 레벨과 타임스템프를 적용하여 병원에서 사용할 수 있는 연합 ID가 생성된다. 그림 2에서 랜덤수는 병원관계자가 replay 공격과 같은 공격에 대응하기 위해서이고 권한레벨은 직원 권한 등급에 따라 환자의 생체정보에 접근할 수 있는 사용자는 제한하기 위해서이다. 타임스탬프는 병원관계자가 사용자의 생체정보에 접근하기 위해 사용되는 정보 중 서명의 유효기간을 위한 정보이다.

3.3 권한확인 및 제어

제안모델에서 병원관계자가 환자의 생체정보를 요청할 경우 인식 제공자가 환자에게 환자의 생체정보 사용에 대한 제공 동의를 요청한 후 병원관계자의 접근레벨에 따라 환자의 생체정보를 제공하는 동작과정은 그림 3와 같다.



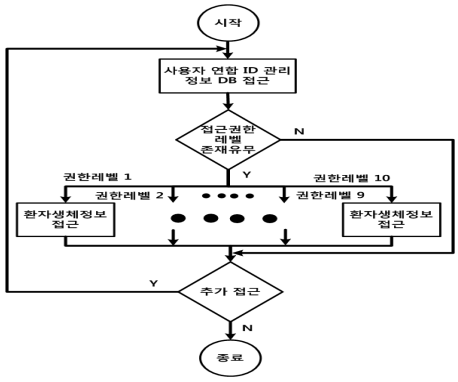
[그림 3] 연합 ID 권한 확인 및 제어 과정

그림 3에서 병원관계자가 환자의 생체정보에 접근하기 위해서는 병원(의사, 간호사, 약사 등)과 환자의 역할에 따라 업무의 권한을 제한받는다. 이 때, 병원관계자의 권한 등급은 사용자의 의료 업무 레벨에 따른 역할로 권한을 부여하고 할당된 권한 등급을 사용하여 환자의 생체정보에 접근할 수 있는 권한을 제한한다. 이 같은 과정을 통하여 사용자 연합 ID 관리정보 데이터베이스를 이용하는 사용자는 업무 시간 및 비용을 절감하면서 의료 서비스를 손쉽게 제공받을 수 있는 기능을 제공받게 된다.

환자의 생체정보에 접근하는 병원관계자는 인증서버를 통해 역할 및 권한을 확인 받을 수 있으며 환자의 생체정보를 요청했을 경우 병원관계자는 이용목적과 병원 청책과 일칠할 경우에만 환자의 생체정보에 접근가능하다. 제안 모델에서는 병원관계자에게 업무분리와 권한 최소화를 통해 환자의 생체정보 유출 및 의료 정보 손실을 예방하고 있다.

3.4 환자기록 접근제어

병원관계자가 환자의 생체정보에 접근하기 위한 동작과정은 그림 4와 같다.



[그림 4] 환자기록 접근제어 순서도

병원관계자가 인식제공자를 통해 환자의 생체 정보에 접근하기 위해서는 우선 병원관계자가 사용자 연합 ID 관리 정보 데이터베이스에 접근하여 병원관계자의 역할에 다른 권한레벨을 부여받아야 한다. 역할에 따른 권한을 부여받은 병원관계자는 권한레벨에 따라 환자의 생체정보에 접근하여 업무를 수행한다. 이 때, 병원관계자가 부여받은 권한레벨을 1부터 10까지이며 숫자가 높을수록 높은 권한을 할당 받는다. 만약 환자의 진찰 기록이 저장되어 있는 기본진료기록 데이터베이스에 낮은 권한으로 접근한다면, 병원관계자는 높은 권한이 요구되는 환자의 생체정보에 대한 접근은 불가능하며, 환자의 병명 및 진료 기록 등 환자의 개인정보 레벨이 낮은 정보만을 볼 수 있다.

환자의 생체정보가 타 병원에서 진찰한 진료기록이 있거나 접근레벨이 높은 특이 질병에 대한 정보가 있을 경우, 병원관계자는 타 병원에게 환자의 정보 공유를 요청한다. 이때, 인식 제공자에게 할당받은 연합 ID를 사용하여 불법적으로 병원관계자의 권한을 남용하는 것을 예방한다. 또한, 제안 모델에서는 병원관계자가 병원에서 정한 보안등급 정책에 따라 업무분리 및 최소한의 권한만을 사용하여 환자의 진료기록에 접근함으로써 환자의 개인정보 유출 및 진료 정보의 손실을 예방할 수 있다.

4. 평가

4.1 내부공격

4.1.1 환자 프라이버시 공격

제안 모델에서는 환자의 프라이버시 공격을 예방하기 위해서 인식 제공자를 통해 연합 ID를 생성한다. 연합 ID는 사용자의 익명 ID와 병원관계자정보를 타임스탬프와 함께 XOR 함으로써 환자 정보를 노출하지 않으면서 환자 정보의 가용성을 보장받을 수 있어 환자의 프라이버시를 보호할 수 있다.

4.1.2 재사용 공격

제 3자가 환자의 생체정보를 얻는 재사용 공격은 인식 제공자가 제공하는 연합 ID를 식 (1)처럼 생성하여 병원관계자가 사용하기 때문에 제3자에게 도청하더라도 안정성을 보장받는다.

연합 ID =사용자 익명 ID ⊕ h(직원번호 ⊕ 랜덤수 ⊕ 권한레벨) ⊕ 타임스탬프 식 (1)

또한, 제안 기법에서는 인식 제공자로부터 전달받은 타임스탬프로 연합 ID를 생성하여 병원관계자가 생성하기 때문에 재사용 공격에 안전한다.

4.1.3 접근 권한에 따른 공격

제안기법은 병원관계자가 환자의 생체정보에 접근하기 위해서 접근권한에 따라 서비스를 허용한다. 만약 권한이 없는 사용자가 환자의 생체정보에 접근할 경우 제안 기법은 환자의 생체정보에 불법적으로 접근하는 것으로 판단하여 서비스를 중단한다. 제안 모델에서는 접근권한에 따라 등록 및 인증 요청, 키 교환, 디바이스 인증 정보 전송, 인증 결과 전송 등이 완료된 후에만 서비스가 정상적으로 제공되기 때문에 신뢰성이 높다.

4.1.4 서비스 거부 공격

제안기법은 서비스 거부 공격을 예방하기 위해서 환자의 생체정보의 접근 제어에 대해서 우선 순위방법을 사용한다. 이 같은 방법은 서버에 접근하는 병원관계자를 손쉽게 관리하기 위함이며 불법 접근 공격이 발생할 경우에는 암호화 기법을 사용하여 서비스 인증 체계를 강화한다.

4.2 외부공격

4.2.1 정보노출 방지

유헬스케어에서 발생하기 쉬운 공격 유형 중 스푸핑 공격은 병원관계자와 환자사이에서 연합 ID를 생성하는데 필요한 정보를 얻음으로써 가능하다. 그러나 제안기법은 인식 제공자와 병원관계자 사이에 전송되는 정보가 연합 ID만을 전송하기 때문에 연합 ID 정보내 정보를 제3가 추출할 수 없어 스푸핑 공격을 수행할 수 없다.

만일 제3자가 연합 ID내 병원관계자의 정보를 얻더라도 제3자는 병원관계자의 정보 h(직원번호 ⊕ 랜덤수 ⊕ 권한레벨) 중 랜덤수를 모르기 때문에 스푸핑 공격이 불가능하다.

4.2.2 정보노출 방지

제안 기법에서는 병원관계자가 환자의 생체정보에 접근할 때문마다 인식 제공자가 생성한 랜덤수를 사용하기 때문에 제 3자에 의해서 병원관계자의 정보가 노출되더라도 제3자가 연합 ID를 불법적으로 생성하여 사용하지 못한다.

4.2.3 DB 정보 유출

제3자에 의해 사용자 연합 ID 관리 정보 데이터베이스가 유출하였다고 가정할 경우, 제3자는 암호화되어 있지 않은 데이터베이스 파일을 쉽게 얻을 수 있다. 그러나, 제안 기법에서는 사용자 연합 ID 관리 정보 데이터베이스에 저장되어 있는 연합 ID를 메번 인식 제공자가 생성한 랜덤수와 타임스탬프로 해쉬하여 생성하기 때문에 연합 ID를 제3가 사용하는 것은 어렵다. 만약 데이터베이스로부터 유출한 정보를 가지고 인증서버에 인증을 요청하더라도 합법적으로 인증을 수행할 수 없어 제안 기법은 안전성을 보장받을 수 있다.

5. 결론

최근 IT 기술이 발전하면서 병원은 인공심장, 전자인식표, 혈액 투속기, 보청기 등의 불치병에 체내삽입장치를 사용하여 환자에게 의료서비스를 제공하고 있다.그러나 병원관계자가 악의적으로 환자의 생체정보를 남용하는 문제점가 점점 증가하는 추세이다. 본 논문에서는 환자의 생체정보를 병원관계자가 남용하는 것을 예방하기

위해서 병원관계자의 권한레벨에 따라 환자의 생체정보에 접근할 수 있는 연합 ID기반의 인증 모델을 제안하였다. 제안된 모델은 연합 ID 관리 시스템 모델에서 기본적으로 제공하는 안전성, 신뢰성, 프라이버시를 기본적으로 제공하면서 서로 다른 인증 식별 체계가 사용되고 있는 병원에서 다양한 형태로 존재하는 다수의 ID 정보를 연합하여 병원 간 건강/의료 정보 공유시 불필요한 개인정보 노출 없이 익명성을 보장받는다. 또한 제안 모델은 권한 레벨에 따라서 접근 허가가 승인되기 때문에 병원관계자 이외에는 환자의 생체정보에 대해서 접근을 허용하지 않기 때문에 제 3자가 쉽게 접근하지 못한다. 향후 연구로 본 연구에서 제안된 모델을 실제 병원업무에 적용한 인증 프로토콜을 연구할 계획이다.

참 고 문 헌

[1] Y. S. Jeong(2012), “RFID-based Authentication Protocol for Implantable Medical Device”, The Journal Of Digital Policy & Management, Vol. 10, No. 2, pp. 141-146.

[2] Y. S. Jeong and S. H. Lee(2012), “u-Healthcare Service Authentication Protocol based on RFID Technology”, The Journal Of Digital Policy & Management, Vol. 10, No. 2, pp. 153-160.

[3] Z. A. Khattak, S. Sulaiman and J. A. Manan(2011), “Security, trust and privacy(STP) framework for federated single sign-on environment”, Proceedings of the 5th International Conference on IT&Multimedia at UNITEN(ICIMU 2011) Malaysia, Vol. 5, pp. 1-6.

[4] K. Bekara, Y. B. Mustapha, S. Bouzefrane, K. Garri, M. Laurent and P. Thoniel(2011), “Ensuring Low Cost Authentication with Privacy Preservation in Federated IMS Environments”, 2011 4th IFIP International Conference on New Technologies, Mobility and Security(NTMS), pp.1-5.

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

[6] Z. A. Khattak, S. Sulaiman and J. A. Manan(2010), “A study on threat model for federated identities in federated identity management system”, 2010 International Symposium in Information Technology(ITSim), Vol. 2, pp. 618-623.

[7] H. Gao, J. Yan and Y. Mu(2010), “Dynamic Trust Model for Federated Identity Management”, 2010 4th International Conference on Network and System Security(NSS), pp. 55-61.

정 윤 수

- 2000년 2월 : 충북대학교 대학원 전자계산학 이학석사
- 2008년 2월 : 충북대학교 대학원 전자계산학 박사
- 2009년 8월~2012년 2월 : 한남대학교 산업기술연구소 전임연구원
- 2012년 3월~현재 : 목원대학교 정보통신공학과 조교수
- 관심분야 : 센서 보안, 암호이론, 정보보호, Network Security, 이동통신보안
- E-Mail : bukmunro@gmail.com