병원 실내 위치기반 의료정보 푸쉬 서비스를 위한 익명 인증 스킴

정회원 안 해 순*, 윤 은 준**,남 인 길***°

An Anonymous Authentication Scheme for Health Information Push Service Based on Indoor Location in Hospital

Hae-Soon Ahn*, Eun-Jun Yoon**, In-Gil Nam***° *Regular Members*

요 약

본 논문에서는 병원 실내 위치기반 의료정보 푸쉬 서비스를 위한 안전하고 효율적인 익명 인증 스킴을 제안한다. 제안한 스킴은 다음과 같은 장점들을 가진다. (1)안전한 일방향 해쉬 함수(secure one-way hash function)를 사용하여 의료 서비스 사용자와 의료 관리센터 사이에 연산 복잡성을 최소화 하였다. (2)의료 관리센터 측에 삽입 공격(insertion attacks) 및 훔친 검증자 공격(stolen-verifier attacks) 등 다양한 암호학적 공격들에 대한 대상이 될 수 있는 민감한 정보를 저장하는 검증 테이블(verification table)을 전혀 필요로 하지 않는다. (3)안전한 상호 인증과 키 설정(secure mutual authentication and key establishment), 기밀 통신(confidential communication), 사용자 프라이버시(user's privacy), 간단한 키 관리(simple key management), 세션 키 독립성(session key independence) 등을 보장하여 높은 보안 수준을 제공한다. 결론적으로 제안한 스킴은 병원 내 실내 위치기반 의료정보 푸쉬 서비스 환경에서 의료 서비스 사용자와 의료 관리센터 사이에서 아주 낮은 연산 오버헤드를 제공하기 때문에 스마트폰과 같은 경량 디바이스를 이용한 다양한 위치기반 의료정보 서비스 환경에 매우 실용적으로 활용될 수 있다.

Key Words : anonymous authentication, u-healthcare, privacy, health information push service

ABSTRACT

This paper proposes a secure and efficient anonymous authentication scheme for health information push service based on indoor location in hospital. The proposed scheme has the following benefits: (1)It is just based on a secure one-way hash function for avoiding complex computations for both health care operations users and health care centers. (2)It does not require sensitive verification table which may cause health care centers to become an attractive target for numerous attacks(e.g., insertion attacks and stolen-verifier attacks), (3)It provides higher security level (e.g., secure mutual authentication and key establishment, confidential communication, user's privacy, simple key management, and session key independence). As result, the proposed scheme is very suitable for various location-based medical information service environments using lightweight-device(e.g., smartphone) because of very low computation overload on the part of both health care operations users and health care centers.

Ⅰ. 서 론

병원 실내 위치기반 의료정보 푸쉬 서비스 시스템에

* 대구대학교 기초교육원 컴퓨터과정(ahs221@hanmail.net), ** 경일대학교 사이버보안학과(ejyoon@kiu.ac.kr)
*** 대구대학교 컴퓨터·IT공학부(ignam@daegu.ac.kr), (° : 교신저자)
논문번호 : KICS2012-01-027, 접수일자 : 2012년 1월 27일, 최종논문접수일자 : 2012년 4월 23일

서의 가장 중요한 문제점은 사용자 프라이버시를 제공하고, 기밀이 보장된 통신망을 이용하여 안전한 상호 인증을 수행할 수 있는지의 여부이다[1-5]. 일반적으로 병원 내 실내 위치기반 의료정보 푸쉬 서비스를 위한 보안 인증 기술에 사용할 수 있는 암호학적 메커니즘들은 공개키 암호시스템(public-key cryptosystem; PKC), 비밀키 암호시스템(secret-key cryptosystems; SKC) 등과 같이 다양한 기술들을 사용할 수 있다[6-10]. 하지만 RSA, ECC와 같은 공개키 암호시스템은 의료 서비스 사용자와 의료 관리센터 사이에서 인증을 위해 사용되며, 두 가지의 단점을 가진다[11-13]. (1)높은 연산 및 통신 오버헤드를 요구한다. (2)PKI 내에 복잡한 공개키 관리가 필요하다. 이러한 PKC를 대신하여 사용할 수 있는 3DES, AES 기반의 비밀키 암호시스템에서의 인증 기술은 PKC에서 문제가 되는 연산 오버헤드를 줄여 줄 수 있으나, SKC 기반의 인증 스킴도 스마트폰과 같은 경량 디바이스 환경에서는 여전히 높은 연산 오버헤드가 발생된다. 요즘 일상적으로 사용하고 있는 센서 기반의 교통 카드, 신분증, 여권, 사원증 등에서 위와 같은 PKC 또는 SKC 기반의 인증 스킴이 활용되지 못하는 이유도 보안 메커니즘들이 높은 연산 오버헤드를 가지기 때문이다. 무엇보다 중요한 것은 병원 내에서 의료 서비스 사용자가 맞춤형 의료정보 푸쉬 서비스를 제공받는 동안 자신에 대한 프라이버시 보장을 위해 익명성 제공이 반드시 이루어져야 한다. 또한 효율성을 너무 고려하게 되면 프라이버시를 보장할 수 없는 등 보안성이 저해될 수 있다. 그러므로 보안성과 효율성을 모두 제공하는 병원 내 실내 위치기반 의료정보 푸쉬 서비스 시스템을 위한 익명성 기반의 인증 기술 개발은 쉽지 않다.

위와 같은 연구 배경을 가지고 본 논문은 다양한 위치에서 각종 의료정보를 손쉽게 확인하고 간편하게 의료 서비스를 받을 수 있도록 하기 위해 의료 서비스 사용자의 위치 인식을 기반으로 의료 서비스를 푸쉬 형태로 제공하는 병원 내 실내 위치기반 의료정보 푸쉬 서비스 시스템을 위한 효율적이고 안전한 익명 인증 스킴을 제안한다. 제안하는 스킴은 다음과 같은 중요한 장점들을 가진다. (1)안전한 일방향 해쉬 함수(secure one-way hash function)를 사용하여 의료 서비스 사용자와 의료 관리센터 사이에 연산 복잡성을 최소화 하였다. (2)의료 관리센터 측에 삽입 공격(insertion attacks) 및 훔친 검증자 공격(stolen-verifier attacks) 등 다양한 암호학적 공격들에 대한 대상이 될 수 있는 민감한 정보를 저장하는 검증 테이블(verification table)을 전혀 필요로 하지 않는다. (3)안전한 상호 인증과 키 설정(secure mutual authentication and key establishment), 기밀 통신(confidential communication), 사용자 프라이버시(user's privacy), 간단한 키 관리(simple key management), 세션 키 독립성(session key independence) 등을 제공하여 높은 보안 수준을 보장한다. 결과적으로, 제안한 인증 스킴은 병원 내 의료 서비스 사용자와 의료 관리센터 사이에서 아주 낮은 연산 오버헤드를 제공하기 때문에 스마트폰과 같은 경량 디바이스를 이용한 병원 내 실내 위치기반 의료정보 푸쉬 서비스 시스템 환경에 매우 실용적으로 활용될 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 병원 실내 위치기반 의료정보 푸쉬 서비스와 관련된 연구를 소개하고, 3장에서는 제안한 병원 실내 위치기반 의료정보 푸쉬 서비스 인증 스킴에 대해 설명한다. 그리고 4장에서는 제안한 인증 스킴에 대한 안전성과 연산 효율성을 분석하고, 5장에서는 본 논문의 결론을 맺는다.

Ⅱ. 관련연구

본 장에서는 병원 의료 서비스 제공 시스템의 기본 개념과 스마트폰과 같은 안전한 의료 서비스 사용자 단말기와 의료 관리센터 간에 통신 링크를 효율적으로 설립하기 위해 필요한 보안 속성들에 대해 소개한다.

2.1 병원 의료 서비스 제공 시스템

그림 1은 제안된 익명 인증 스킴이 적용되는 병원 의료 서비스 제공 시스템에 대한 설명도이다[14,15]. 그림 1에 도시된 바와 같이, 제안된 익명 인증 스킴이 적용되는 병원 의료 서비스 제공 시스템은 먼저 의료 서비스를 이용하려는 사용자가 병원 입구에 들어서면 병원 입구에 설치된 Access Point(AP)에 자동으로 접속하게 되고 의료 관리센터는 DB에 저장된 자료를 바탕으로 병원의 간단한 소개와 접수 여부를 묻는 메시지, 기존의 진료기록, 예약현황 등의 서비스 목록을 푸쉬 형태로 의료 서비스 사용자 단말기인 스마트폰에 전송한다. 메시지를 전송받은 의료 서비스 사용자는 병원 접수 등 추가 서비스를 요청할 수 있다.

여기서, 각 AP는 내과, 외과, 소아과 등과 같은 진료실 근처에 각각 위치하고 있으므로 의료 서비스 사용자가 각 진료실 근처로 이동하면 기존의 AP와 연결이 끊어지고 해당 진료실 근처에 있는 AP에 다시 자동으로 접속하게 된다. 이때 의료 관리센터는 항상 DB에 저장된 자료를 바탕으로 해당 AP의 위치정보를 이용하여 의료진 정보(이력, 경력), 해당 진료실에 대한 예약, 대기자 수, 진료시간 등 해당 위치에 특화된 서비스

메시지 목록을 푸쉬 형태로 전송한다. 상기 메시지를 전송받은 의료 서비스 사용자는 추가 서비스를 간편하게 요청할 수 있다.

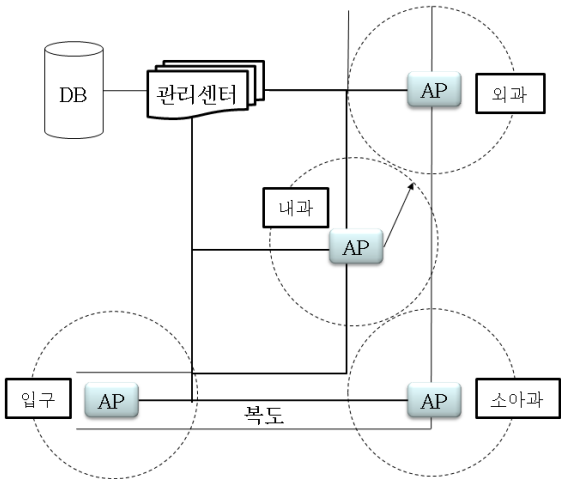

그림 1. 병원 의료 서비스 제공 시스템
Fig 1. Hospital Healthcare Service Providing System

2.2 병원 실내 위치기반 의료정보 푸쉬 서비스 시스템

현재 병원은 점점 대형화되는 추세로 병원 내에서 환자들이 자신들의 위치를 잃어버리는 경우가 많고, 이로 인해 원하는 의료서비스를 신속하게 제공받기 어렵다. 이러한 문제를 해결하기 위해 병원 실내 위치기반 의료정보 푸쉬 서비스 시스템을 이용하여 이동통신 인터페이스를 가지고 있는 의료 서비스 사용자의 단말기가 AP 커버리지에 의해 구분되는 위치기반 서비스 존(service zone) 내에 위치할 경우 의료정보 메시지나 서비스목록 메시지 등 해당 서비스 존에 특화된 다양한 위치기반 의료정보 서비스를 제공받는다면 환자들은 쉽고 편리하게 병원 진료를 받을 수 있을 것이다. 또한, 병원 내 실내 위치기반 의료정보 푸쉬 서비스 시스템은 병원 곳곳에 설치된 AP의 위치 정보를 이용해 의료관리센터의 데이터베이스에 저장된 환자의 개인 의료정보(진료기록, 예약사항 등), 의료진 정보(경력, 이력 등) 및 병원 안내사항 등 각종 의료정보를 의료 서비스 사용자의 단말기에 간편하게 수신할 수 있다.

기존의 병원 의료 서비스에서 병원에 환자가 처음 내원했을 때 접수를 위해 환자의 이름, 성별, 나이, 주민번호와 같은 신상정보를 컴퓨터로 입력받아 데이터베이스화하기 위해서는 환자가 직접 의료기관의 접수처로 가서 접수를 해야 하는 불편이 있다. 또한 각 진료과목에 대해 의료진의 정보, 기존 진료 기록 등 환자가 원하는 정보를 쉽게 얻기 힘들다. 그리고 다양한 진료과목에서 환자를 통합적으로 관리하기 때문에 하나의 진료과목에서 간단한 의료 서비스를 원하는 환자들에게는 의료기관 이용의 효율성이 떨어진다.

최근 들어, 이동통신 단말기인 스마트폰의 사용이 급증하고 있으며 다양한 무선 인터넷 서비스에 대한 수요도 증가하고 있다. 무선 인터넷 서비스는 여러 가지가 있지만, 그 중 대표적인 것이 위치기반 서비스라고 할 수 있다. 종래에는 이동통신 가입자가 위치한 곳에 특화된 서비스를 제공하기 위해 이동통신망의 셀 기반 방식과 GPS(Global Positioning System) 방식이 주로 활용되어 왔다. 그러나, 상기 방식들은 의료 서비스 사용자가 일차적으로 서비스에 대한 요청을 해야 하며, 원하는 정보를 얻기 위해서는 복잡한 과정이 필요하다는 불편함이 있다. 따라서 의료 서비스 사용자 단말기가 주변 AP에 자동으로 접속하면 미리 저장되어 있는 해당 AP의 위치를 이용해 의료 관리센터의 데이터베이스에 저장된 환자의 개인 의료정보(진료기록, 예약사항 등), 의료진 정보(경력, 이력 등) 및 병원 안내사항 등 해당 위치에 특화된 각종 의료정보 메시지 목록을 푸쉬 형태로 전송하고 의료 서비스 사용자는 수신된 메시지 목록을 이용하여 간편하게 가능한 서비스를 요청할 수 있는 시스템이 필요한 것이다.

병원 내 실내 위치기반 의료정보 푸쉬 서비스 시스템은 위치인식을 이용한 병원 의료 서비스 제공 방법에 있어서 서비스 제공을 위한 각종 데이터를 수집하는 데이터 수집 단계, 접속한 AP의 위치정보를 이용해 병원 내에서 의료 서비스 사용자 단말의 위치를 확인하는 단계, 데이터베이스를 통해 확인된 위치정보에 대응하는 의료 정보 메시지를 확인 또는 추출하는 단계, 확인 또는 추출된 의료정보 메시지를 의료 서비스 사용자 단말기인 스마트폰에 푸쉬 형태로 전송하는 단계와 전송받은 메시지를 스마트폰에 출력 되도록 하는 단계로 구성된다. 그림 2는 본 논문에서 적용되는 의료 서비스 사용자 단말, 의료 관리센터 간의 메시지 송수신 과정을 개략적으로 도시한 흐름도이다. 먼저 애플리케이션을 사용하는 사용자가 해당 서비스를 이용하기 위해서는 로그인 과정이 필요하다. 이는 (1)의료 서비스 사용자가 스마트폰에서 의료 관리센터로 로그인 Request를 보내고 (2)의료 관리센터에서 스마트폰으로 로그인 성공 또는 실패 Response를 보냄으로써 이루어진다. 다음으로 (3)스마트폰이 근처 AP에 자동으로 접속되면 (4)의료 관리센터에서 스마트폰으로 해당 위치에 특화된 의료 서비스 메시지 목록을 전송한다. (5)메시지 목록을 전송받은 의료 서비스 사용자는 원하는 서비스 Request를 의료 관리센터에게 요청할 수 있으

며, (6)의료 관리센터는 해당 서비스의 Response를 의료 서비스 사용자에게 전송한다.

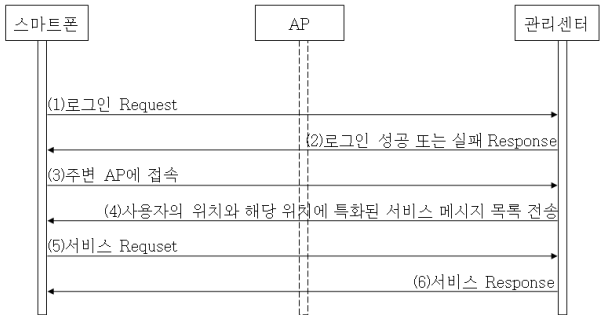

그림 2. 의료 서비스 사용자 단말기(스마트폰)와 의료 관리센터 간의 메시지 송수신 과정
Fig 2. Message Exchange Process between Healthcare Service User (Smartphone) and Healthcare Management Center

2.3 요구되는 필수적인 속성(required essential properties)

위 그림 2에서 보여주듯이 스마트폰 의료 서비스 사용자, AP들 그리고 의료 관리센터 간의 통신들은 대기 중에 열려있다고 가정한다. 이와 같은 가정 하에 아래와 같은 필수적인 보안 속성들이 효율적인 통신 링크 설정 및 다양한 암호학적 공격들을 예방하기 위한 고려사항들 이다[16-22].

(1) 상호인증(mutual authentication): 의료 서비스 사용자와 의료 관리센터 간의 상호 인증은 필수적인 보안 요소이다. 의료 관리센터를 위한 적절한 인증이 없으면, 의료 서비스 사용자는 의료 서비스 사용자 인증 단계에서 자신에게 정보를 보내는 미확인 상대방에 의한 위장 공격(impersonation attack)에 속거나, 합법적인 의료 관리센터에 의해 인식되지 않은 서비스들이 설정된 통신망을 통해 제공됨으로써 메시지 무결성을 저해할 수 있게 된다.

(2) 기밀 통신(confidential communication): 무선 경로상의 통신은 엿보기 또는 도청이 쉽다. 보안 프로토콜은 공유된 세션키를 사용한 암호화를 통해 의료 서비스 사용자와 의료 관리센터 간에 송수신되는 통신 메시지들에 대한 기밀성을 반드시 보장해야 한다.

(3) 사용자 프라이버시(user's privacy): 이동 네트워크에서 프라이버시 보호를 위해 꼭 고려되어야 하는 두 가지 중요한 점은 사용자 식별자(user identity)와 위치(location) 정보이다. 때때로 사용자의 실제 식별자(real identity)는 공격자들에게 아주 중요한 정보이며, 사용자와 연결 가능한 식별자는 해당 사용자의 행동 패턴을 분석하는 데 중요한 단서가 되기 때문에 사용자의 식별자 및 이와 연관된 정보들은 병원 내에 이동 중인 사용자의 현재 위치 정보와 마찬가지로 외부 공격자로 부터 안전하게 보호되어야 한다.

(4) 저가의 연산 비용과 업데이트 비용(low computation and update cost): 보안 프로토콜은 낮은 연산 비용을 제공해야 한다. 한정된 자원을 가지는 의료 서비스 사용자의 휴대용 장치에는 복잡한 계산을 기반으로 하는 보안 프로토콜은 적합하지 않으며 빈번한 계산과 업데이트로 인해 의료 관리센터에 병목현상(bottleneck)을 일으킬 수 있다. 따라서 본 속성은 PCS와 MSCS에서의 스마트폰과 같은 경량 휴대용 장치뿐만 아니라 의료 관리센터에서 반드시 고려되어야 하는 속성이다.

(5) 간편한 키 관리(simple key management): 다양한 비밀 키 탈취 공격들로부터 비밀 키를 보호하는 것은 보안과 관련된 모든 환경에서 아주 중요하기 때문에 가능한 한 비밀 키 관리(secret key management)는 공격자의 공격에 대해 반드시 보호되어야 한다. 비밀 키 관리 문제를 편리하게 하기 위해서는 첫째 합법적인 사용자와 공유된 비밀 키들을 저장하고 있는 보안상 민감한 테이블을 서버 측에 두지 않아야 하며, 둘째 공개키 기반의 연산 오버헤드가 높은 보안 방법을 모바일 기반의 GSM 및 UMTS와 같은 실용적인 응용 환경에 적용하는 것을 가급적 피해야 한다.

(6) 최소 신뢰성(minimum trust): 병원 내에서 합법적인 의료 서비스 사용자들이 이동할 때 의료 관리센터로 부터 서비스를 제공받기 위해 자신들의 개인 정보를 등록하기 때문에 의료 관리센터는 높은 신뢰성을 가져야 한다. 하지만 관련된 다른 제3자의 신뢰 수준은 가능한 낮게 지정해야 높은 사용자 프라이버시를 제공할 수 있다.

(7) 세션 독립성(session independence): 공유된 비밀 세션 키는 항상 위협받을 가능성이 높다. 공격자가 알려진 키 공격(known key attacks)이라 불리는 공격 기법을 사용하게 되면 이들 세션 키들과 공격으로 부터 얻은 세션 키 간의 상관관계를 이용하여 이전 세션 또는 다음 세션으로부터

비밀 키를 유도할 수 있다. 유출된 세션 키가 보안성 유지에 영향을 주는 것을 피하기 위해 세션 키는 일회성 변수 개념으로 구하고 사용되어야 한다. 이러한 기법은 위장 또는 재전송 공격들을 예방할 수 있다.

Ⅲ. 제안한 익명 인증 스킴

본 장에서는 제안한 의료 관리센터와 의료 서비스 사용자가 동시에 세션 키를 공유하는 병원 내 실내 위치기반 의료정보 푸쉬 서비스를 위한 안전하고 효율적인 익명 인증 스킴에 대해 설명한다. 제안한 스킴에서 초기화 과정으로 SHA-2 또는 SHA-256과 같은 안전한 일방향 해쉬 함수 기반의 암호 시스템을 설정한다[23]. 그리고 의료 관리센터에 의료 서비스 사용자가 등록을 하게 되면, 의료 관리센터는 의료 관리센터가 가지고 있는 개인 비밀 키(long-term private key)를 이용하여 의료 서비스 사용자를 위한 인증 토큰(authentication token)을 생성하고 사용자의 마스터 키(master key)를 유도한다. 마스터 키는 의료 관리센터 측에서 의료 관리센터가 가지고 있는 개인 비밀 키로부터 계산된다.

의료 관리센터와 통신하기 전에, 의료 서비스 사용자는 메시지 인증 코드(message authentication code, MAC)를 계산하고 의료 관리센터에 보낸다. MAC 코드를 받은 즉시, 의료 관리센터는 수신된 MAC을 검증하기 위해 의료 서비스 사용자의 마스터 키를 복구하여 검증한다. 만약 검증에 통과되면, 의료 관리센터는 의료 서비스 사용자의 마스터 키와 이와 대응되는 임시 식별자(temporary identity)로부터 사용자와 공유되는 세션 키를 유도한다. 이후 의료 관리센터는 사용자가 다음 인증 단계에서 사용할 수 있도록 새로운 임시 식별자를 생성하여 이전에 계산된 세션 키를 사용하여 암호화한다. 암호화된 메시지는 응답으로서 MAC와 함께 의료 서비스 사용자에게 전송된다. 사용자는 수신한 MAC의 유효성을 검사하여 올바르면 해당 스킴에 대한 인증을 성공적으로 수행하게 되어 인증을 종료한다. 명확한 것은 제안한 스킴은 PKC, SKC, PKI가 필요없을 뿐만 아니라 사용자 장치 내에 저장되는 어떠한 인증서도 요구하지 않는다. 제안한 스킴은 등록(registration)과 인증(authentication)의 2단계로 구성된다. 본 논문에서 사용되는 용어는 표 1과 같이 정의된다.

표 1. 용어 정의
Table 1. Notations

기호	의 미
U, MC	의료 서비스 사용자와 의료 관리센터로 명명되는 두 통신 당사자들
U_{ID}, T_{ID}, AP_{ID}	의료 서비스 사용자의 식별자(*ID*), 사용자의 임시 식별자, AP의 식별자
x	의료 관리센터의 장기 개인 키(long-term private key)
X -> Y:M	통신 당사자 X가 다른 통신자 Y에게 메시지 M을 송신
$h(\cdot)$	SHA-2나 SHA-256]와 같은 안전한 일방향 해쉬 함수
MACk(·)	키 k를 기반으로 하는 메시지 인증 코드
$\oplus$	배타적 논리합(XOR; eXclusive OR) 연산

3.1 의료 서비스 사용자 등록단계(registration phase)

그림 3은 제안하는 인증 스킴의 의료 서비스 사용자 등록 단계를 보여준다. 의료 관리센터 MC는 자신의 장기 개인 키 x를 소유한다고 가정한다. 등록 단계 동안 의료 서비스 사용자 U는 시스템으로부터 합법적인 의료 서비스 사용자가 되기 위해 요청을 하면 의료 관리센터 MC는 아래 과정을 통해 의료 서비스 사용자 등록을 수행한다.

R1. U **-> MC:** U_{ID}

의료 서비스 사용자 U는 자신의 식별자 U_{ID}를 자유롭게 선택한 후 안전한 통신 채널을 통해 MC에게 제출한다.

R2. MC -> U: Smart card(T_{ID}, key)

시스템에서 식별자 U_{ID}를 가지는 각 사용자 U를 위해 MC는 해당 세션에서 성공적인 인증 이후 다음 세션에서의 인증을 위해 사용할 수 있는 초기화된 임시 식별자 T_{ID}를 결정한다. 이후, MC는 마스터 키 key=$h(U_{ID}, x)$를 생성한다. MC는 사용자의 스마트카드에 {T_{ID}, key}를 저장하고, 안전한 통신 채널을 통해 사용자에게 발급해 준다. 마지막으로 MC는 V= $U_{ID} \oplus h(T_{ID}, x)$를 계산하고 인증 테이블 내에 {V, T_{ID}}를 저장한다. 이 과정은 공격자가 검증 테이블에서 위조된 검증 항목을 삽입하는 삽입 공격을 방어할 수 있다.

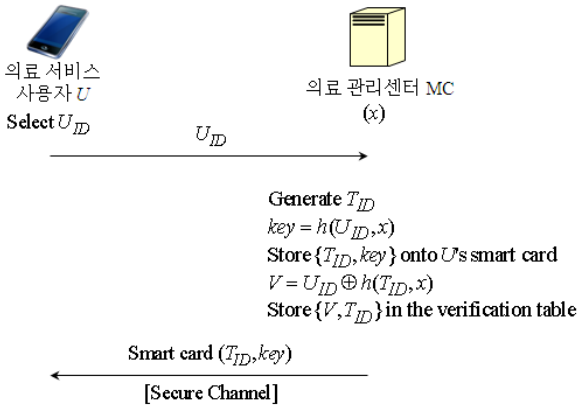

그림 3. 의료 서비스 사용자 등록 단계
Fig 3. Healthcare Service User Registration Phase

3.2 의료 서비스 사용자 인증 단계 (authentication phase)

그림 4는 본 논문에서 제안하는 스킴에서 인증 단계를 보여준다. 인증 단계 동안 의료 서비스 사용자 U는 의료 관리센터 내의 자원에 접근하고 서비스를 받기 전에 반드시 인증을 받아야만 한다. 제안하는 스킴의 인증단 계에서 AP와 MC간의 통신 채널은 SSL 프로토콜과 TLS 프로토콜과 같은 보안 암호 기술들을 기반으로 안전한 통신 채널이 설정되어 있다고 가정한다[24]. 인증 단계는 다음과 같이 수행된다.

A1. U -> AP: T_{ID}, mac$U$

만약 사용자 U가 AP 또는 MC와 함께 세션 키 sk 협상을 원한다면, U는 자신의 이동 장비를 이용하여 다음과 같은 과정을 수행한다.

(a) 자신의 스마트폰과 같은 이동 장비 내의 스마트 카드를 사용하여 로그인 인증 소프트웨어를 실행한 후 자신의 식별자 U_{ID}를 입력한다.

(b) 세션 키 sk=h(key, T_{ID})를 계산한다. 여기에서 T_{ID}는 타임스탬프 값으로 성공적인 로그인이 수행한 후에 갱신된다.

(c) 메시지 인증 코드 mac$U$=MACkey(U_{ID}, sk)를 계산하고 T_{ID}와 함께 AP에게 전송한다.

A2. AP -> NCC: T_{ID}, macU, AP_{ID}

사용자 U로 부터 인증 메시지를 받은 즉시, AP는 자신의 식별자 AP_{ID}를 추가하여 MC에게 전달한다.

A3. MC -> AP: c, macNCC, AP_{ID}

AP로부터 인증 메시지를 받은 즉시 MC는 AP의 정당성을 AP_{ID}를 통해 검증한 후 다음과 같은 과정을 수행한다.

(a) 검증 테이블을 검색하여 T_{ID}와 연관된 대응 정보 V={V, T_{ID}}를 찾는다. 여기에서 V= $U_{ID} \oplus h(T_{ID}, x)$ 값이다.

(b) 자신의 장기 비밀 키 x와 수신한 T_{ID}를 사용하여 $h(T_{ID}, x)$를 계산한다.

(c) 다음과 같은 V$\oplus h(T_{ID}, x)$ 연산을 수행하여 사용자 U의 식별자 $U_{ID}^{'}$를 추출한다.

$V \oplus h(T_{ID}, x) = U_{ID} \oplus h(T_{ID}, x) \oplus h(T_{ID}, x) = U_{ID}^{'}$

(d) 추출된 $U_{ID}^{'}$와 세션키 sk'=h(key', T_{ID})를 이용하여 사용자의 마스터 키 key'=$h(U_{ID}^{'}, x)$를 계산한다.

(e) mac'U=MAC$_{key}$'($U_{ID}^{'}$, sk')를 계산하고, mac'U와 수신한 mac$U$를 검증한다. 만약 두 값이 일치하면 U는 인증되고 세션 키도 검증된다. 만약 두 값이 틀리면 인증 요청은 거부된다.

(f) 새로운 임시 식별자 T_{IDnew}를 생성하고 다음 인증을 위해 검증 테이블 내에 있는 이미 사용한 과거의 T_{ID}를 새로운 T_{IDnew}로 업데이트 한다.

(g) c=h(sk)$\oplus T_{IDnew}$와 macNCC=MAC'sk(T_{IDnew})를 계산한 후 AP에게 {c, macNCC, AP_{ID}}를 송신한다.

A4. AP -> U: c, macNCC

AP는 c와 macNCC를 사용자에게 전송한다.

A5. 사용자 U는 c와 macNCC를 수신하면, 자신의 c와 sk를 사용하여 다음과 같은 c$\oplus$sk 계산을 통해 새로운 임시 식별자 T_{IDnew}를 추출한다.

$$\mathbf{c \oplus sk} = h(\mathbf{sk'}) \oplus T_{IDnew} \oplus \mathbf{sk} = T_{IDnew}^{'}$$

의료 서비스 사용자 U는 mac'NCC=MAC'sk($T_{IDnew}^{'}$)를 계산하고, mac'NCC와 macNCC를 검증한다. 만약 두 값이 일치하면 이동 의료 서비스 사용자는 MC가 자신을 검증하여 자신의 식별자를 정확히 알고 있음을 확인하고, 다음 인증을 위해 T_{ID}를 T_{IDnew}로 대체하게 된다. 이 과정에서 세션키 sk에 대한 상호 검증도 이루어진다. 사용자 U와 MC는 설정된 현 세션 내에서 교환되는 기밀 정보를 보호하기 위해 일회용 세션 키 sk=h(key, T_{ID})를 사용한다.

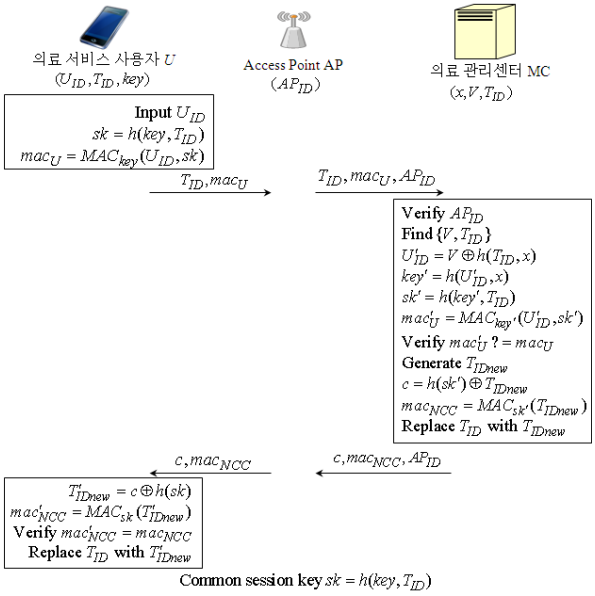

그림 4. 의료 서비스 사용자 인증 단계
Fig 4. Healthcare Service User Authentication Phase

Ⅳ. 안전성과 효율성 분석

본 장에서는 제안한 스킴의 인증 단계 수행 과정에서 병원 실내에서의 진료실 간의 이동 의료 서비스 사용자 *U*와 의료 관리센터 MC에 대한 안전성과 효율성에 대해 살펴본다.

4.1 안전성 분석

본 논문에서 제안한 인증 스킴은 표 2에서 보여주는 것과 같이 안전한 상호 인증, 메시지 기밀성, 사용자 프라이버시를 제공할 뿐만 아니라 낮은 연산 비용, 간편한 키 관리, 최소 신뢰성 그리고 세션 키 독립성을 제공한다.

(1) 상호 인증(mutual authentication): 제안한 스킴의 인증 단계 <A3>에서 의료 관리센터 MC는 mac'*U*=MACkey'(U'_{ID}, sk')를 계산한 후 mac'*U*와 이용자 *U*로부터 수신한 mac*U*를 검증한 후 AP에게 {c, macNCC, AP_{ID}}를 송신하면 AP는 의료 서비스 사용자 *U*에게 {c, macNCC, AP_{ID}}를 송신한다. 의료 서비스 사용자 *U*는 <A5> 단계에서 mac'NCC=MAC'sk(T'_{IDnew})를 계산한 후 수신한 macNCC와 mac'NCC를 검증한다. 만약 두 값이 일치하면 이동 의료 서비스 사용자 *U*는 MC가 자신을 검증하여 자신의 식별자를 정확히 알고 있음을 확인하고, 다음 인증을 위해 T_{ID}를 T_{IDnew}로 대체하게 된다. 그러므로 이 인증 단계 과정에서 세션키 sk에 대한 상호 검증도 이루어짐으로써 제안한 인증 스킴은 상호 인증을 보장한다.

(2) 기밀성: 무선 경로상의 통신은 공격자의 엿보기 또는 도청 공격이 쉽게 이루어진다. 따라서 공유된 세션키를 사용한 암호화를 통해 의료 서비스 사용자와 의료 관리센터 간에 송수신되는 통신 메시지들에 대한 기밀성을 반드시 보장해야 한다. 제안한 스킴에서는 식별자 T_{ID}를 의료 서비스 사용자 *U*와 의료 관리센터 MC 둘 다 안전하게 공유하고 있다. 또한 사용자 *U*와 의료 관리센터 MC 모두 mac'*U*=MAC$_{key}$'(U'_{ID}, sk')를 계산하고, mac'*U*와 수신한 mac*U*를 검증한다. 만약 두 값이 일치하면 *U*는 인증되고 세션 키를 검증한 후 새로운 임시 식별자 T_{IDnew}를 생성하고 다음 인증을 위해 검증 테이블 내에 있는 이미 사용한 과거의 T_{ID}를 새로운 T_{IDnew} 값으로 업데이트함으로써 기밀성을 제공한다.

표 2. 제안한 스킴의 보안성 및 성능
Table 2. Security and Performance of the Proposed Scheme

보안성	제안스킴
상호 인증	제공함
기밀성	제공함
사용자 프라이버시	제공함
낮은 통신 비용	제공함
간편한 키 관리	제공함
최소 신뢰성	제공함
세션 독립성	제공함

(3) 사용자 프라이버시: 이동 네트워크에서 프라이버시 보호를 위해 꼭 고려되어야 하는 두 가지 중요한 점은 사용자 식별자와 위치 정보이다. 그러므로 제안한 스킴에서는 태그 식별자 T_{ID}를 의료 서비스 사용자 *U*와 의료 관리센터 MC 둘 다 안전하게 공유하고 있을 뿐만 아니라 태그 식별자를 포함하고 있는 송수신되는 통신 메시지를 상호 인증을 수행한다. 그리고 세션 키를 검증한 후에는 매 세션마다 새로운 임시 식별자 T_{IDnew}를 생성하고 다음 인증을 위해 검증 테이블 내에 있는 이미 사용한 과거의 T_{ID}를 새로운 T_{IDnew} 값으로 업데이트 한다. 이와 같은 이유로 제안한 스킴은 태그 소유자의 이동 경로를 파악할 수 없게 됨으로써 태그 정보에 대한 사용자 프라이버시를 보호한다.

(4) 저가의 연산 비용과 업데이트 비용: 한정된 자원을 가지는 의료 서비스 사용자의 휴대용 장치에는 복

잡한 연산을 기반으로 하는 보안 프로토콜은 적합하지도 않을 뿐더라 무엇보다 연산 비용을 줄여야 한다. 따라서 본 논문에서 제안한 스킴은 높은 연산 오버헤드를 발생시키는 RSA, ECC와 같은 공개키 암호시스템 및 3DES, AES 기반의 비밀키 암호시스템에서의 인증 기술을 전혀 사용하지 않고 안전한 일방향 해쉬 함수와 메시지 인증 코드 연산만을 사용함으로써 통신 라운드 수를 줄이고 연산 비용과 업데이트 비용을 줄였다.

(5) 간편한 키 관리: 비밀 키 유출 공격을 방지하고, 비밀 키를 보호하는 것은 보안과 관련된 매우 중요한 요소이다. 비밀 키 관리 문제를 편리하게 해결하기 위해서 본 논문에서는 공유된 비밀 키를 관리하는 테이블을 서버측에 두지 않았으며, 의료 서비스 사용자와 의료 관리센터에서 각각 비밀 키를 공유하는 방법을 사용하였다. 또한 공개키 기반의 연산 오버헤드가 높은 보안 방법을 사용하지 않았으므로 간편한 키 관리를 제공한다.

(6) 최소 신뢰성: 의료 서비스 사용자들은 의료 관리센터로 부터 서비스를 제공받기 위해 자신들의 개인정보를 등록하므로 의료 관리센터는 반드시 높은 신뢰성을 가져야 한다. 그에 반해 관련된 다른 제3자의 신뢰 수준은 가능한 매우 낮게 지정해야 높은 사용자 프라이버시를 제공할 수 있다. 따라서 제안한 스킴에서는 제3자의 최소 신뢰성 유지를 위해 <A3> 단계에서 의료 관리센터 MC는 mac'U=MACkey'($U_{ID}^{'}$, sk')를 계산한 후 mac'U와 이용자 U로부터 수신한 mac$U$를 검증한 후 AP에게 {c, macNCC, AP_{ID}}를 송신하면 AP는 의료 서비스 사용자 U에게 {c, macNCC, AP_{ID}}를 송신한다. 그런 다음 의료 서비스 사용자 U는 <A5> 단계에서 mac'NCC=MAC'sk($T_{IDnew}^{'}$)를 계산한 후 수신한 macNCC와 mac'NCC를 검증하고 태그 식별자를 업데이트함으로써 제3자의 최소 신뢰성을 유지한다.

(7) 세션 독립성: 의료 서비스 사용자와 의료 관리센터간에 공유된 비밀 세션 키는 항상 위협받을 가능성이 높다. 공격자는 키 공격으로 획득한 세션 키 간의 상관관계를 이용하여 이전 세션 또는 다음 세션으로부터 비밀 키를 유도할 수 있으므로 제안한 스킴에서는 세션키 sk에 대한 상호 검증을 수행하고, 의료 서비스 사용자 U와 의료 관리센터 MC는 설정된 현 세션 내에서 교환되는 기밀 정보를 보호하기 위해 일회용 세션 키 sk=h(key, T_{ID})를 사용하여 세션 독립성을 제공한다.

4.2 효율성 분석

기존의 인증 스킴에서는 RSA, ECC와 같은 공개키 암호시스템은 의료 서비스 사용자와 의료 관리센터 사이에서 인증을 위해 사용되었다. 그러나 높은 연산량 및 통신 오버헤드가 발생되고, PKI 내에 복잡한 공개키 관리가 필요하다는 단점이 있다. 이러한 PKC를 대신하여 사용할 수 있는 3DES, AES 기반의 비밀키 암호시스템에서의 인증 기술을 사용하여 PKC에서 문제가 되는 연산 오버헤드를 줄였지만 SKC 기반의 인증 스킴도 스마트폰과 같은 경량 디바이스 환경에서는 여전히 높은 연산 오버헤드가 발생된다. 따라서 본 논문에서는 공개키 암호시스템과 비밀키 암호시스템에서와 같은 인증 기술을 배제한 안전한 일방향 해쉬 함수 연산과 인증 코드(MAC) 연산만을 사용하였다. 제안한 인증 스킴의 연산량은 표 3에서 보여주는 것과 같이 의료 서비스 사용자 U측에서 1번의 해쉬 함수 연산과 2번의 메시지 인증 코드 연산만을 필요로 하고, 의료 관리센터 MC 측에서는 4번의 해쉬 연산과 2번의 메시지 인증 코드 연산만을 요구하기 때문에 낮은 연산량을 수행함을 알 수 있다. 또한 통신 라운드 수는 2번이며 결론적으로 제안한 스킴의 인증 수행 과정에서 통신비용이 낮아 스마트폰과 같은 의료 서비스 사용자의 휴대 단말기를 이용한 병원 내 실내 위치기반 의료정보 푸쉬 서비스 환경에 매우 적합함을 알 수 있다.

표 3. 제안한 스킴의 연산 효율성
Table 3. Computational Efficiency of the Proposed Scheme

	의료 서비스 사용자 U	의료 관리센터 MC	전체 연산량
일방향 해쉬 연산	1	4	5
MAC 연산	2	2	4
통신 라운드 수	2		

Ⅵ. 결 론

본 논문에서는 병원 실내 위치기반 의료정보 푸쉬 서비스를 위한 안전하고 효율적인 익명 인증 스킴을 제안하였다. 제안한 스킴은 다음과 같은 장점들을 가진다. (1)안전한 일방향 해쉬 함수를 사용하여 의료 서비스 사용자와 의료 관리센터 사이에 연산 복잡성을 최소화 하였다. (2)의료 관리센터 측에 삽입 공격 및 훔친 검증자 공격 등 다양한 암호학적 공격들에 대한 대상이 될 수 있는 민감한 정보를 저장하는 검증 테이블을 전혀 필요로 하지 않는다. (3)안전한 상호 인증과 키 설

정, 기밀 통신, 사용자 프라이버시, 간단한 키 관리, 세션 키 독립성 등을 제공함으로써 높은 보안 수준을 제공한다. 결과적으로 제안한 인증 스킴은 병원 내 실내 위치기반 의료정보 푸쉬 서비스 환경에서 사용자의 프라이버시를 보장할 뿐만 아니라 의료 서비스 사용자와 의료 관리센터 사이에서 매우 낮은 연산 오버헤드를 제공하기 때문에 스마트폰과 같은 사용자의 경량 디바이스를 이용한 다양한 위치기반 의료정보 서비스 환경에 아주 실용적으로 활용될 수 있다. 또한 위치 기반 의료 정보 제공 시스템에서 사용자들이 가지고 있는 휴대단말기의 이동하는 위치에 따라 대응되는 의료 정보를 실시간으로 수신할 수 있기 때문에 무엇보다 사용자의 편의성이 크게 증대될 것으로 기대된다.

참 고 문 헌

[1] Gostin LO, Turek-Brezina J, Powers M, Kozloff R, Faden R, Steinauer DD. Privacy and Security of Personal Information in a New Health Care System. JAMA. 270(20), 2487-2493 (1993)

[2] J. Kim, A. R. Beresford, and F. Stajano, Towards a Security Policy for Ubiquitous Healthcare Systems, Proc. 1st International Conference on Ubiquitous Convergence Technology, 263-272 (2006)

[3] S.-D. Bao, Y.-T. Zhang, and L.-F. Shen, Physiological Signal Based Entity Authentication for Body Area Sensor Networks and Mobile Healthcare Systems, Proc. 27th Annual International Conference of Engineering in Medicine and Biology Society, 2455-2458 (2005)

[4] M. Markovic, Z. Savic, and B. Kovacevic, Secure mobile health systems: principles and solutions, M-Health: Emerging Mobile Health Systems, Kluwer Academic Publishers, 81-106 (2007)

[5] A. Boukerche and R. Yonglin, A secure mobile healthcare system using trust-based multicast scheme. IEEE J. Selected Areas Comm. 27(4), 387-399 (2009)

[6] B Schneier, Applied Cryptography, 2nd edn. (Wiley, New York, 1996)

[7] N. Koblitz, Elliptic curve cryptosystems, in Mathematics of Computation 48, 203-209 (1987)

[8] C Ellison, B Schneier, Ten risks of PKI: what you're not being told about public-key infrastructure. Comput. Secur. J. 16(1), 1-7 (2000)

[9] H. Wang, B. Sheng, Q. Li, Elliptic curve cryptographybased access control in sensor networks, Int. J. Security and Networks. 1(3/4), 127-137 (2006)

[10] X. H. Le, S. Lee, I. Butun, M. Khalid, R. Sankar, M. Kim, M-H. Han, Y-K. Lee, H. Lee. An Energy-Efficient Access Control Scheme for Wireless Sensor Networks based on Elliptic Curve Cryptography. Journal of Communications and Networks. 11(6), 599-606 (2009)

[11] F. Amin, A. H. Jahangir, and H. Rasifard. Analysis of Public-Key Cryptography for Wireless Sensor Networks Security. World Academy of Science, Engineering and Technology 41, 529-534 (2008)

[12] X. H. Le, R. Sankar, M. Khalid, and S. Lee, Public Key Cryptography - based Security Scheme for Wireless Sensor Networks in Healthcare, 4th International Conference on Ubiquitous Information Management and Communication (ICUIMC), Suwon, Korea, (January 2010)

[13] W. Joppe, M. Kaihara, T. Kleinjung, A. K. Lenstra, and P. Montgomery, On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography Cryptology, Report on Cryptology ePrint Archive, 389 (2009)

[14] HJ Lee, SH Lee, KS Ha, HC Jang, WY Chung, JY Kim, YS Chang, DH Yoo. Ubiquitous healthcare service using Zigbee and mobile phone for elderly patients. International Journal of Medical Informatics. 78(3), 193-198 (2009)

[15] A. Boukerche, Ren. Yonglin. A secure mobile healthcare system using trust-based multicast scheme. IEEE Journal on Selected Areas in Communications. 27(4), 387-399 (2009)

[16] TH Chen, WB Lee, HB Chen, A self-verification authentication mechanism for mobile satellite communication systems. Comput. Electr. Eng. 35(1), 41-48 (2009)

[17] GA Safdar, MP O'Neill, Performance analysis of novel randomly shifted certification authority authentication protocol for MANETs. EURASIP J. Wirel. Commun. Netw. 2009 Article ID 243956, 1-11 (2009)

[18] R Jian, L Yun, L Tongtong, SPM: source privacy

for mobile ad hoc networks. EURASIP J. Wirel. Commun. Netw. 2010 Article ID 534712, 1-10 (2010)

[19] V Vijay, O Diethelm, S Jaleel, JH Antoni, J Sanjay, Broadcast secrecy via key-chain-based encryption in single-hop wireless sensor networks. EURASIP J. Wirel. Commun. Netw. 2011 Article ID 695171, 1-12 (2011)

[20] JM Li, YH Park, X Li, A USIM-based uniform access authentication framework in mobile communication. EURASIP J. Wirel. Commun. Netw. 2011 Article ID 867315, 1-12 (2011)

[21] JY Huang, IE Liao, HW Tang, A forward authentication key management scheme for heterogeneous sensor networks. EURASIP J. Wirel. Commun. Netw. 2011 Article ID 296704, 1-10 (2011)

[22] EJ Yoon, KY Yoo, JW Hong, SY Yoon, DI Park, MJ Choi. An efficient and secure anonymous authentication scheme for mobile satellite communication systems. EURASIP Journal on Wireless Communications and Networking. 86, 1-15 (2011)

[23] N Sklavos, O Koufopavlou, Implementation of the SHA-2 hash family standard using FPGAs. J. Supercomput. 31(3), 227{248 (2005)

[24] R Oppliger, R Hauser, D Basin, SSL/TLS session-aware user authentication. IEEE Comput. 41(3), 59{65 (March 2008)

안 해 순 (Hae-Soon Ahn) 정회원

1996년 2월 경일대학교 컴퓨터공학과(공학사)
2001년 경일대학교 컴퓨터공학과(공학석사)
2010년 대구대학교 컴퓨터정보공학과(공학박사)
2004년~2008년 경일대학교 컴퓨터공학부 전임강사
2008년~현재 대구대학교 기초교육원 컴퓨터과정 초빙교수
<관심분야> 데이터베이스, 정보보안, 데이터베이스 보안, RFID 보안

윤 은 준 (Eun-Jun Yoon) 정회원

2003년 경일대학교 컴퓨터공학과(공학석사)
2007년 경북대학교 컴퓨터공학과(공학박사)
2007년~2008년 대구산업정보대학 컴퓨터정보계열 전임강사
2008년~2011년 경북대학교 전자전기컴퓨터학부 연구교수
2011년~현재 경일대학교 사이버보안학과 조교수
<주관심분야: 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜>

남 인 길 (In-Gil Nam) 정회원

1978년 경북대학교 전자공학과(공학사)
1981년 영남대학교 전자공학과(공학석사)
1992년 경북대학교 전자공학과(공학박사)
1978년~1981년 대구은행 전산부
1980년~1990년 경북산업대학 부교수
1990년~현재 대구대학교 컴퓨터·IT공학부 교수
<관심분야> 데이터베이스, 데이터베이스 보안, RFID 보안