의료정보보호를 위한 RFID를 이용한 환자 인증 시스템

정회원 윤 은 준*, 유 기 영**°

Patient Authentication System for Medical Information Security using RFID

Eun-Jun Yoon*, Kee-Young Yoo**° *Regular Members*

요 약

최근 의료 과실을 줄이기 위한 방법으로 RFID 기술을 많이 적용한다. 이 기술을 이용하면 환자들에 대한 의료 처방 및 치료를 정확하게 수행 할 수 있다. 의료 환경에서 RFID 기술 활용의 핵심은 프라이버시 제공이다. 본 논문에서는 위와 같은 환경을 기반으로 안전하고 효율적으로 환자 인증 및 환자 개인 의료 정보를 보호할 수 있는 RFID 인증 시스템을 제안한다. 제안한 시스템은 RFID 기반의 환자 인증 프로토콜과 데이터베이스 보안 프로토콜로 구성된다. 결론적으로, 제안한 RFID 인증 시스템은 강인한 보안성과 효율성을 제공하여 주어, u-Hospital 및 u-Healthcare 같은 첨단 의료 환경 상에서 환자 인증뿐만 아니라 환자 개인의 의료 정보를 안전하게 보호할 수 있음으로 실용적으로 사용되어 질 수 있다.

Key Words : RFID, Authentication, Ubiquitous Security, Medical Information Security

ABSTRACT

Recently, RFID technology can successfully be used to reduce medical errors. This technology can aid in the accurate matching of patients with their medications and treatments. The enthusiasm for using RFID technology in medical settings has been tempered by privacy concerns. In this paper, we propose a secure and efficient RFID authentication system to not only authenticate patients' authenticity but also protect patients' personal medical informations. The proposed system consists of RFID-based patient authentication protocol and database security protocol. As a result, since the proposed RFID authentication system provides strong security and efficiency, it can be used practically for patient authentication and personal medical information protection on the high technology medical environments such as u-Hospital and u-Healthcare.

Ⅰ. 서 론

최근 미국에서는 불필요한 수술(Unnecessary Surgery), 잘못된 약물 처방(Wrong Medications), 또는 약물 이상 반응(Adverse Drug Reactions) 등의 의료 과실로 인해 한해에 12만여명 이상이 목숨을 잃고 있음이 조사되었다. 이러한 의료 과실의 상당 부분은 환자를 올바르게 식별하지 않았거나, 환자에 대한 약물 처방이 올바르게 이루어지지 않아서 발생하였다[1-3].

첨단 의료 환경 상에서 위와 같은 의료 과실을 줄이기 위한 방법으로 환자의 의료 프로필(Profile)을 이용하여 정확하게 환자를 식별할 수 있도록 RFID (Radio Frequency IDentification) 기술을 많이 적용하

※ 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2010-0010106).
* 경북대학교 대학원 전자전기컴퓨터학부(ejyoon@knu.ac.kr)
** 경북대학교 IT대학 컴퓨터공학부 정보보호연구실(yook@knu.ac.kr) (° : 교신저자)
논문번호 : KICS2010-03-124, 접수일자 : 2010년 3월 29일, 최종논문접수일자: 2010년 6월 5일

고 있다. 일반적으로 의료 환경에서의 RFID 기술은 초단파나 장파의 무선 주파수를 이용하여 환자의 의료정보를 물리적인 접촉 없이 비접촉 방식으로 읽거나 정보를 기록할 수 있는 최첨단 기술로 정의할 수 있다[1-3]. 이로 인해 RFID 기술은 USN(Ubiquitous Sensor Network) 기술과 더불어 유비쿼터스 컴퓨팅(Ubiquitous Computing) 환경 실현을 위한 중요한 핵심 기술로 가장 주목을 받고 있는 기술이다[4-6]. 의료 환경에서 위와 같은 RFID 기술을 이용하면 환자들에 대한 의료처방 및 치료를 정확하게 수행 할 수 있다.

일반적으로 RFID 시스템은 리더(Reader), 태그(Tag) 그리고 백-엔드 데이터베이스(Back-end Database)의 3가지 구성요소로 이루어 져있다. 리더와 백-엔드 데이터베이스의 연산 능력에 비해 RFID 태그는 연산 능력이 떨어지며, 객체를 유일하게 식별하기 위한 정보만을 가지며, 정보 노출, 위치 추적 등으로 인한 개인의 프라이버시(Privacy) 침해를 유발할 수 있는 문제점을 지니고 있다[4-22]. 따라서 의료 환경에서 RFID 기술 활용을 위해 반드시 고려되어야 할 핵심은 프라이버시(Privacy) 제공 여부이다.

본 논문에서는 위와 같은 의료 환경을 기반으로 안전하고 효율적으로 환자 인증 및 환자 개인 정보를 보호할 수 있는 RFID 인증 시스템을 제안한다. 제안한 RFID 시스템은 RFID 기반의 환자 인증 프로토콜과 데이터베이스 보안 프로토콜[23]로 구성된다. 결론적으로, 제안한 RFID 인증 시스템은 강인한 보안성과 효율성을 제공하여 주어, u-Hospital 및 u-Healthcare 같은 첨단 의료 환경에서 환자 개인의 프라이버시 제공 및 정보 보호를 위해 실용적으로 사용되어 질 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 RFID 시스템과 일반적인 RFID 인증 시스템들이 만족해야 할 보안 요구사항에 관해 설명한다. 3장에서는 본 논문에서 제안한 RFID 기반의 환자 인증 시스템을 기술하고, 4장과 5장에서 각각 안전성과 효율성을 분석 및 제안 시스템에 대한 검토를 한다. 최종적으로 6장에서 결론을 맺는다.

Ⅱ. 배경 지식

본 장에서는 RFID 시스템 환경과 일반적인 RFID 인증 프로토콜이 만족해야 할 보안 요구사항에 관해 살펴본다.

2.1 RFID 시스템 구성요소 및 동작원리

일반적으로 RFID 시스템은 그림 1과 같이 백-엔드 데이터베이스 서버(DB), RFID 리더(Reader), RFID 태그(Tag)들의 3종류의 컴포넌트들로 구성되어 진다[1-22].

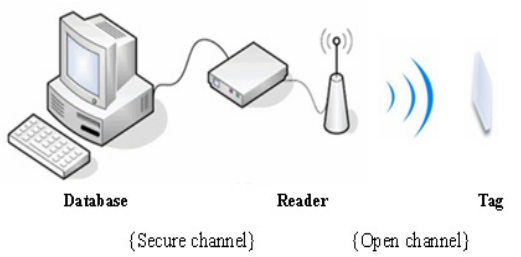

그림 1. RFID 시스템 구성요소

DB 서버는 각 태그를 위한 식별자(*ID*), 비밀키(k)와 제품 정보 등 필요한 정보 집합을 관리하고 있으며, 각 태그는 읽고 쓰기가 가능한 메모리를 내장하고 있다. DB 서버와 리더 간의 채널은 일반적으로 안전한 채널(Secure Channel)이며 리더와 태그 간의 채널은 안전하지 않은 채널(Insecure Channel)로 가정한다. 따라서 리더와 태그 사이의 주고받는 모든 통신 메시지들은 공격자에 의해 엿보기나 수정이 가능하다.

일반적인 RFID 시스템의 동작 원리는 다음과 같다. 먼저, 리더는 태그에게 질의(Query) 정보를 전송한다. 제품에 대한 고유의 식별자 정보를 가지고 있는 태그는 리더의 요청에 의해 자신의 식별자 정보를 리더에게 전송한다. 리더는 태그가 보내오는 식별자 정보를 수신한 후, DB 서버에게 전달한다. DB 서버는 자신의 DB 테이블 정보와 리더로부터 수신한 정보를 이용하여 태그를 인증한 후, 해당 태그에 관한 제품 정보 등을 리더에게 알려준다.

2.2 보안 요구사항들[1-22]

일반적으로 RFID 시스템은 다음과 같은 보안 문제들을 고려하여 설계되어져야 한다.

2.2.1 그 익명성(Tag Anonymity)

태그의 식별자(*ID*)는 평문 형태로 전송 되지 않아야 하며, 태그와 리더 사이의 통신 채널 상으로부터 쉽게 계산되어지지 않아야한다.

2.2.2 위치 프라이버시(Location Privacy)

태그와 리더 사이의 통신 메시지 내용으로부터 태그의 식별자(*ID*)를 추적(Trace)할 수 없어야 한다.

2.2.3 재전송 공격(Replay Attack)

수동적 공격자가 과거에 리더와 태그 사이에 통신

한 내용들을 도청한 후 이를 재전송하여 합법적인 태그, 리더 또는 DB로 인증을 받으려는 공격이다.

2.2.4 스푸핑 공격(Spoofing Attack)

공격자가 정당한 태그로 위장하여 리더로부터 인증에 필요한 정보를 획득하거나, 정당한 리더로 위장하여 태그 또는 DB로부터 인증에 필요한 정보를 획득하거나, 또는 정당한 DB로 위장하여 리더로부터 인증에 필요한 정보를 획득하여 이를 이용하여 정당한 태그, 리더 또는 DB로 인증 받는 공격이다.

2.2.5. 위치 트래킹 공격(Location Tracking Attack)

공격자가 태그의 위치변화를 감지함으로 인해 태그 소유자의 이동 경로를 파악하여 사용자의 프라이버시(privacy)를 침해하는 공격이다.

Ⅲ. 제안한 RFID 기반 환자 인증 시스템

본 장에서는 안전한 환자 인증 및 환자 개인의 의료 정보 보호를 위한 RFID 기반 환자 인증 시스템을 제안한다. 표 1은 본 논문에서 사용되는 시스템 파라미터들을 보여준다.

표 1. 시스템 파라미터

용 어	정 의
Tag	환자가 착용하고 있는 RFID 태그
Reader	의사가 소지하고 있는 RFID 리더
DB	의료정보 백-엔드 데이터베이스
query	*Tag*의 응답을 요청하는 리더의 요청
TID	*Tag*에게 할당된 고유 ID 정보
k_{TID}	*Tag*의 고유 비밀키
k_{DB}	*DB*의 고유 비밀키
$h()$	안전한 일방향 해쉬 함수(hash function)
$M_{k_{DB}}()$	k_{DB}를 이용한 메시지 인증 코드(MAC)
time	*Reader*가 생성한 타임스탬프 값
prng()	의사난수생성기
T_{rand}	*Tag*가 생성한 랜덤 값
$\oplus$	배타적 논리합(XOR;eXclusive OR) 연산
$\|$	연접 연산(concatenation) 연산
$A \rightarrow B: X$	X가 A에서 B로 전송

3.1 시스템 환경

제안한 RFID 기반 환자 인증 프로토콜에서는 병원 내의 모든 환자들이 자신들의 의료 정보를 식별할 수 있는 RFID 태그를 전자팔찌(Bracelet) 또는 전자발찌(Ankles) 등의 스마트 밴드(Smart Band) 형태로 착용하고 있음을 가정한다[1-3]. 또한 병원 내의 RFID 백-엔드 데이터베이스와 병원 내의 의사 또는 간호사가 소지하고 있는 리더 간의 통신 채널(Communication Channel)은 안전한 채널(Secure Channel)임을 가정하며, 각 환자 태그의 비밀 키 k_{TID}는 병원 내 백-엔드 데이터베이스에 DB 암호화 알고리즘을 통해 안전하게 등록되어 있음을 가정한다[23].

3.2 의료 DB 정보 암호화

본 절에서는 RFID 시스템 환경에서 병원 내의 DB 서버에 저장할 환자의 중요한 의료 비밀 정보를 암호화하는 기법을 제안한다. 환자에 관한 비밀 정보를 DB 내에 저장 시에는 안전성뿐만 아니라 저장 효율성을 고려하여 저장 및 관리하여야 한다. 그림 2는 제안한 의료 DB 정보 암호화 방법을 보여주고 있다. DB 내의 태그 비밀키인 k_{TID}를 안전하게 암호화(Encryption)하여 저장하는 방법은 다음과 같이 동작한다.

(1) 병원(DB)는 환자(태그)의 식별자인 *TID*와 자신의 비밀키 K_{DB}를 이용하여 고유한 MAC 값인 m 비트열 길이의 $M_{k_{DB}}(TID)$ 값을 계산한다.

(2) 병원(DB)는 환자(태그)의 비밀키인 k_{TID}와 위에서 구한 MAC(Message Authentication Code) 값인 $M_{k_{DB}}(TID)$를 $k_{TID} \oplus M_{K_{DB}}(TID)$와 같이 비트 단위 XOR 연산을 수행하여, 암호화된 환자(태그) 비밀키 값인 $C_{TID} = k_{TID} \oplus M_{k_{DB}}(TID)$를 계산한 후, DB 테이블 내의 해당 환자(태그)의 비밀키 필드에 저장한다.

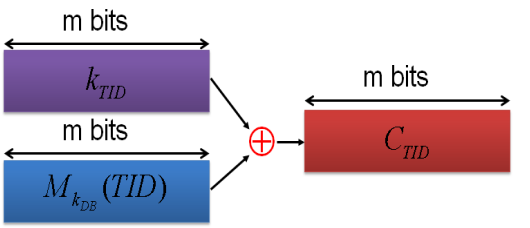

그림 2. DB 내의 환자(태그) 비밀키 암호화

3.3 환자 인증

그림 3은 제안한 RFID 기반 환자 인증 프로토콜의 구성과 동작 과정을 보여주며, 다음의 5단계를 거쳐 인증 과정이 이루어진다. 여기에서 병원(리더)는 의사 또는 간호사가 소지한 리더기를 의미한다.

(1) 병원(리더)→환자(태그): $\{Query, Time\}$

병원(리더)는 타임스탬프 $time$을 생성한 후, 환자(태그)에게 $Query$와 함께 전송한다. 여기에서 타임스탬프 $Time$은 시간 동기화(Time Synchronization)를 위한 목적이 아니라 해당 환자(태그)가 병원 반경 내에 있는 지 여부를 리더가 빨리 검증하기 위해 사용된다.

(2) 환자(태그)→병원(리더): $\{H_{TID}, T_{rand}, Time\}$

환자(태그)는 랜덤 값 T_{rand}를 $prng()$로부터 생성한 후, 병원(리더)로부터 수신한 $Time$과 자신의 식별자인 TID 및 비밀 키 k_{TID}를 함께 이용하여 랜덤 해쉬 값 $H_{TID} = h(k_{TID} \| TID \| T_{rand} \| Time)$을 계산한 후, 병원(리더)에게 계산된 H_{TID}를 T_{rand} 및 $Time$과 함께 전송한다.

(3) 병원(리더)→병원(DB): $\{H_{TID}, T_{rand}, Time\}$

병원(리더)는 먼저 수신한 메시지가 자신이 정한 임계 시간(Threshold Time) 내에 도착하였는지 여부를 수신한 $Time$을 이용하여 검증한다. 만약 검증을 통과하여 환자(태그)가 병원 반경 내에 존재함이 확인되면, 수신한 메시지들을 병원(DB)에게 전송한다.

(4) 병원(DB)→병원(리더): $\{Info\}$

병원(DB)는 병원(리더)로부터 전송받은 $\{H_{TID}, T_{rand}, Time\}$와 자신의 데이터베이스 내에 저장하고 있는 모든 TID와 k_{TID} 쌍을 이용하여 병원(리더)로부터 수신한 H_{TID} 값과 일치하는 TID와 k_{TID} 쌍을 검색한다. 만약 일치하는 값이 검색되지 않으면, 해당 환자(태그)가 존재하지 않는다는 오류(error) 메시지를 병원(리더)에게 전송하고, 만약 일치하는 값이 검색되면 해당 환자(태그)를 인증하고 환자(태그)에 대한 의료 관련정보(related information)인 $Info$를 병원(리더)에게 전송한다.

(5) 병원(리더)는 병원(DB)로부터 수신한 값이 오류일 경우, 환자(태그)와의 통신을 중단하고, 정상적인 인증이 되었을 경우에서는 병원(DB)로부터 수신한 의료 관련정보(related information)인 $Info$를 활용하여 해당 환자(태그)에 대해 원하는 의료 업무를 수행한다.

3.4 의료 DB 정보 복호화

제안한 환자 인증 프로토콜의 (4)단계에서, 병원(리더)로부터 임의의 환자(태그)에 대한 인증 요청 메시지를 수신한 병원(DB)는 암호화된 환자(태그) 정보에 대한 빠른 검색을 위해 다음의 과정을 수행하여 병원(DB) 내의 환자(태그) 비밀키인 k_{TID}를 안전하게 복호화(Decryption)하여 안전하게 환자(태그) 인증을 수행하게 된다.

(1) 병원(DB)는 DB 테이블 내의 환자(태그) 식별자 저장 필드와 암호화된 비밀키 값 저장 필드로부터 식별자 TID와 $C_{TID} = k_{TID} \oplus M_{k_{DB}}(TID)$를 읽어온다.

(2) 병원(DB)는 TID와 자신의 비밀키 k_{DB}를 이용하여 고유한 MAC 값인 m 비트열 길이의 $M_{k_{DB}}(TID)$ 값을 계산한다.

(3) 병원(DB)는 C_{TID}와 $M_{k_{DB}}(TID)$를 이용하여 $C_{TID} \oplus M_{k_{DB}}(TID)$와 같이 비트 단위 XOR 연산을 수행하여 태그의 비밀키 k_{TID}를 얻는다. 여기에서 C_{TID}는 $k_{TID} \oplus M_{k_{DB}}(TID)$이므로 아래와 같이 k_{TID}가 복원되는 것을 쉽게 알 수 있다.

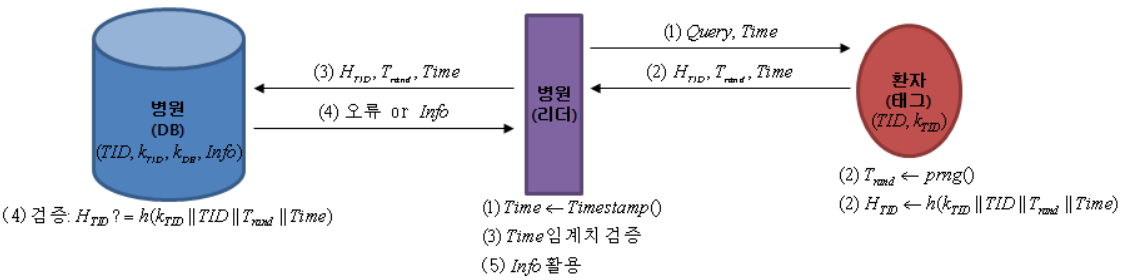

그림 3. 제안한 RFID 기반 환자 인증 프로토콜

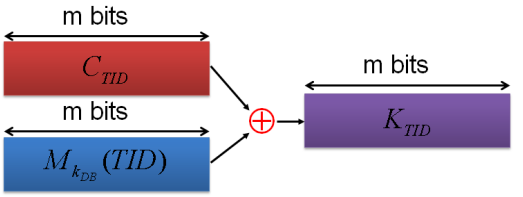

그림 4. DB 내의 환자(태그) 비밀키 복호화

$$C_{TID} \oplus M_{k_{DB}}(TID)$$
$$= k_{TID} \oplus M_{k_{DB}}(TID) \oplus M_{k_{DB}}(TID)$$
$$= k_{TID}$$

(4) 병원(DB)는 복호화하여 얻은 k_{TID}를 이용하여 병원(리더)로부터 수신한 메시지의 합법성 검증을 통하여 환자(태그)를 인증하게 된다.

Ⅳ. 안전성 분석

본 장에서는 제안한 RFID 기반 환자 인증 시스템에 대한 보안성 분석을 한다. 먼저, 제안한 인증 시스템의 안전성 분석을 위해 필요한 중요한 보안 항목을 다음과 같이 정의한다[24,25].

[정의 1] *강력한 비밀 키(k_{TID}와 k_{DB})는 높은 엔트로피(entropy)를 가지는 값으로써 다항식 시간(polynomial time) 내에 계산되어 질 수 없다.*

[정의 2] *안전한 일방향 해쉬 함수(secure one-way hash function) $y = h(x)$와 안전한 메시지 인증 코드 함수 $y = M(x)$에서, 주어진 x를 이용하여 y를 계산하는 것은 쉽지만, 주어진 y를 이용하여 x를 계산하는 것은 어렵다.*

위 정의들을 기반으로 제안한 RFID 인증 시스템은 다음과 같이 재전송 공격, 스푸핑 공격, 위치 트래킹 공격, 태그 키 유출 공격, DB 정보 유출 공격에 안전하며 태그 익명성을 제공한다.

4.1 재전송 공격(Replay attack)

공격자는 임의의 세션에서 병원(리더)와 환자(태그) 사이에서 전송되는 정보를 모두 도청한 후, 다음 세션에서 정당한 병원(리더)나 환자(태그)로 위장을 시도하는 재전송 공격을 수행할 수 있다. 하지만 제안한 RFID 인증 시스템에서는 매 세션마다 병원(리더)가 생성하는 새로운 타임스탬프 $Time$와 환자(태그)가 생성하는 새로운 랜덤 값 T_{rand}를 이용하여 병원(DB)에 의해 인증을 수행하기 때문에, 과거에 공격자에 의해 재전송된 랜덤 값들은 병원(DB)의 인증 과정 중에 쉽게 검출됨으로 재전송 공격을 수행할 수 없다.

4.2 스푸핑 공격(Spoofing attack)

공격자가 병원(DB)와 환자(태그) 간에 공유된 비밀키인 k_{TID}를 얻을 수 있으면, 병원(리더) 또는 환자(태그)로의 스푸핑 공격을 성공할 수 있다. 하지만 위 [정의 1]과 [정의 2]에 의해 제안한 RFID 인증 시스템에서 공개 통신 채널 상으로 전송되는 정보들인 $\{Time, H_{TID}, T_{rand}\}$을 이용하더라도, 공격자는 병원(DB)와 환자(태그) 내에 각각 안전하게 저장하고 있는 비밀 키인 k_{TID}를 직접적으로 얻을 수 있는 방법이 없게 되어 스푸핑 공격을 수행할 수 없다.

4.3 위치 트래킹 공격(Location tracking attack) 및 위치 프라이버시(Location privacy)

환자(태그) 측에서 생성하는 랜덤 값 T_{rand}는 매 세션마다 다른 값으로 생성되기 때문에 이로부터 계산된 $H_{TID} = h(k_{TID} \| TID \| T_{rand} \| Time)$ 또한 매 세션마다 변경된다. 따라서 공격자는 현재 세션에서 환자(태그)의 응답이 과거 세션에 도청한 응답과 동일한지를 쉽게 구별할 수 없다. 이로 인해, 공격자는 태그의 이동경로를 쉽게 추적을 할 수 없을 뿐만 아니라, 특정한 태그를 식별할 수 없기에 위치 트래킹 공격을 수행할 수 없게 되어 위치 프라이버시를 제공할 수 있다.

4.4 DB 정보 유출 공격(DB information exposure attack)

모든 환자(태그)들의 비밀키 정보를 저장하고 있는 병원(DB) 내의 환자(태그) 관리 테이블이 유출되었다고 가정하자. 기존의 RFID 인증 시스템에서는 이러한 DB 유출로 인해 임의의 공격자는 암호화되어 있지 않는 DB 테이블로 부터 간단히 모든 환자(태그)들의 비밀키 k_{TID}를 쉽게 얻을 수 있다. 하지만 제안한 의료 DB 보안 프로토콜 상에서는 공격자가 환자(태그)의 비밀키 정보를 담고 있는 DB 테이블을 얻더라도 해당 환자(태그)의 비밀키 k_{TID}가 아닌 암호화된 $C_{TID} = k_{TID} \oplus M_{k_{DB}}(TID)$를 얻게 된다. C_{TID}는 병원(DB)의 비밀키인 k_{DB}로 암호화되어 있기 때문에 이를 모르고서는 C_{TID}로부터 환자(태그)의 비밀키 k_{TID}를 복호화할 수 없다. 결론적으로 제안한 의료 DB 정보 보안 프로토콜은 임의의 공격자에 의한 DB

유출 공격에 안전하다. 더 나아가, 만약 합법적인 한 환자(태그)의 비밀키 k_{TID}를 알고 있는 공격자라 하더라도 $C_{TID} = k_{TID} \oplus M_{k_{DB}}(TID)$로부터 $C_{TID} \oplus k_{TID}$를 계산하여 $M_{k_{DB}}(TID)$는 얻을 수는 있지만, 위 [정의 1]과 [정의 2]에 의해 병원(DB)의 비밀키인 k_{DB}는 여전히 얻을 수 없음으로, 나머지 환자(태그)들의 비밀키에 대한 안전성을 여전히 보장할 수 있게 되어 제안한 의료 DB 정보 보안 프로토콜은 합법적인 임의의 태그에 의한 DB 유출 공격에 대해서도 안전하다.

4.5 태그 익명성(Tag anonymity)

병원(리더)는 타임스탬프 $Time$을 생성하여 환자(태그)에게 전송하고, 환자(태그)는 수신한 $Time$과 자신이 생성한 임의의 랜덤 값 T_{rand} 그리고 식별자인 TID와 비밀 키인 k_{TID}를 이용하여 안전한 일방향 해쉬 함수의 도움으로 $H_{TID} = h(k_{TID} \| TID \| T_{rand} \| Time)$을 계산한 후 병원(리더)에게 전송한다. 이로 인해, H_{TID}을 도청한 공격자는 환자(태그)의 비밀 키인 k_{TID}를 알지 않고서는 환자(태그)의 식별자인 TID를 추측할 수 없을 뿐만 아니라, 일방향 해쉬 함수의 성질에 의해 H_{TID}로부터 환자(태그)의 TID 정보를 직접적으로 얻을 수 없게 됨으로 환자(태그)의 익명성을 제공할 수 있다.

Ⅴ. 효율성 분석 및 검토

본 장에서는 표 2와 같이 제안한 RFID 기반 환자 인증 시스템에 대한 효율성을 분석한다.

제안된 RFID 인증 시스템은 환자(태그) 측에서 하나의 랜덤 값 생성이 요구되며, 병원(DB) 측에서는 DB 보안 기법을 사용하지 않으면 n번의 해쉬/MAC 연산이 요구되며, DB 보안 기법을 사용하면 $2n$번의 해쉬/MAC 연산이 요구된다. 환자(태그)와 달리 병원(DB)는 높은 시스템 성능과 연산 능력을 가짐으로 n번 또는 $2n$번의 해쉬/MAC 연산을 통한 환자(태그) 인증은 빠른 시간 내에 이루어 질 수 있다. 결론적으로 RFID 기반 환자 인증 시스템은 안전성과 효율성 및 실용성을 제공함을 알 수 있다.

표 2. 효율성 분석

컴포넌트 / 비교요소	병원(DB)		병원(리더)	환자(태그)
	DB보안(X)	DB보안(O)		
랜덤 값	0	0	0	1
타임스탬프	0	0	1	0
해쉬/MAC 연산	n	$2n$	0	1
XOR 연산	0	n	0	0
통신 라운드 수	4			

n : 병원(DB) 서버 내에 저장된 최대 환자(태그)수

특히 제안하는 시스템의 RFID 인증 프로토콜은 기존의 해쉬-체인(Hash-Chain) 기반의 RFID 인증 프로토콜들이 태그 측에서 최대 n번의 해쉬 연산을 수행하는 비효율적인 문제점을 해결하기 위해 태그 측에서 한번의 해쉬 연산 만을 수행하여 동일한 안전성을 제공할 뿐만 아니라 높은 효율성을 보장할 수 있도록 설계하였다. 또한 재전송 공격 등을 방지하기 위해 리더 측에서만 타임스탬프 값을 생성함으로 시간 동기화 문제도 없다. 더 나아가 본 논문에서는 기존의 RFID 인증 프로토콜들에서는 고려하지 않은 백-엔드 데이터베이스 서버 내에 저장된 태그들의 비밀 정보들을 안전하게 보호하기 위한 DB 정보 암호화 기법을 제안하였다. 접근 제어 기법을 기반으로 하는 기존 DBMS의 정보 암호화 방식은 내부자 또는 악의적인 공격자에 의한 DB 정보 유출 또는 해킹시 해당 테이블로부터 평문의 태그 비밀 정보를 직접적으로 얻을 수 있어 위 안전성 분석에서 설명하였던 다양한 공격들에 취약할 수 있다. 이러한 DB 정보 유출 공격에 대한 보안성을 제공하기 위해 최근 안전한 키워드 검색(Secure Keyword Search) 기법 등의 연구로 활발히 연구가 진행되고 있기에 본 논문에서 제안한 DB 정보 암호화 기법은 반드시 필요한 보안 기술로 환자 개인 정보 보호를 위해 다양하게 응용 및 사용되어 질 수 있다.

Ⅵ. 결론 및 향후연구

본 논문에서는 의료 과실을 줄여주며 정확한 환자의 개인 의료 정보를 활용할 수 있게 하는 RFID 기반의 환자 인증 시스템을 제안하였다. 제안한 인증 시스템은 안전하고 효율적으로 환자 인증 및 환자 개인의 의료 정보를 보호할 수 있으며, 데이터베이스 보안 프로토콜적용을 통하여 보다 높은 보안성을 제공할 수 있다. 결론적으로, 제안한 RFID 인증 시스템은 강인한 보안성과 효율성을 제공하여 주어, 첨단 의료 환경 상에서 환자에 대한 안전한 인증뿐만 아니라 환자 개인의 의료 정보를 안전하게 보호할 수 있음으로, u-Hospital 및 u-헬스케어와 같은 첨단 의료 환경에서 환자 개인의 프라이버시 제공 및 의료 정보 보호를 위

해 실용적으로 사용되어 질 수 있다. 향후 연구로는 제안한 환자 의료 정보 보호를 위한 RFID 기반 환자 인증 시스템을 개발을 통한 실용성 증명에 목표를 둔다.

참 고 문 헌

〔1〕 B. Starfield, "Is US health really the best in the world?," Journal of the American Medical Association, Vol.284, No.4, pp.483-485, 2000.

〔2〕 J. A. Fisher, "Indoor positioning and digital management: emerging surveillance regimes in healthcare," In T. Monahan (Ed), Surveillance and Security: Technological Politics and Power in Everyday Life, New York: Routledge, pp.7788, 2006.

〔3〕 M. Anshel and S. Levitan, "Reducing medical errors using secure RFID technology," ACM SIGCSE Bulletin, Vol.39, No.2, pp.157-159, 2007.

〔4〕 F. Klaus, "RFID handbook," Second Edition, Jone Willey & Sons, 2003.

〔5〕 S. A. Weis, "Security and privacy in radio-frequency identification devices," MS Thesis. MIT. May, 2003.

〔6〕 S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," Security in Pervasive Computing 2003, LNCS 2802, pp.201-212, Springer-Verlag Heidelberg, 2004.

〔7〕 S. E. Sarma, S. A. Weis, D. W. Engels. "RFID systems, security & privacy implications," White Paper MIT-AUTOID-WH_014, MIT AUTO-ID CENTER, 2002.

〔8〕 A. Juels and R. Pappu, "Squealing euros: privacy protection in RFID-enabled banknotes," In proceedings of Financial Cryptography-FC'03, Vol.2742 LNCS, pp.103-121, Springer-Verlag, 2003.

〔9〕 A. Juels, R. L. Rivest, M Szydlo "The blocker tag: selective blocking of RFID tags for consumer privacy," In Proceedings of 10th ACM Conference on Computer and Communications Security, CCS 2003, pp. 103-111, 2003.

〔10〕 S. Junichiro, H. Jae-Cheol and S. Kouichi, "Enhancing privacy of universal re-encryption scheme for RFID tags," EUC 2004, Vol.3207 LNCS, pp.879-890, Springer-Verlag, 2004.

〔11〕 S. A. Weis, S. Sarma, R. Rivest, D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," Security in Pervasive Computing 2003, LNCS 2802, pp.201-212, Springer-Verlag, 2004.

〔12〕 M. Ohkubo, K. Suzuki, and S. Kinoshita, "Hash-chain based forward-secure privacy protection scheme for low-cost RFID," Proceedings of the SCIS 2004, pp.719-724, 2004.

〔13〕 양형규, 안영화, "유비쿼터스 컴퓨팅 환경에 적합한 RFID 인증 프로토콜에 관한 연구," 전자공학회논문지, 제42권, 제CI-1호, pp.45-50, 2005.

〔14〕 김진목, 유황빈, "유비쿼터스 환경에서 Pre-Distribution을 기반으로 한 안전한 RFID 시스템," 전자공학회논문지, 제42권, 제CI-6호, pp.29-36, 2005.

〔15〕 오선문, 강대성, "NMF와 LDA 혼합 특징추출을 이용한 해마 학습기반 RFID 생체 인증 시스템에 관한 연구," 전자공학회논문지, 제43권, 제SP-4호, pp.46-54, 2006.

〔16〕 박인정, 현택영, "RFID를 이용한 작업관리 시스템," 전자공학회논문지, 제44권, 제CI-2호, pp.31-36, 2007.

〔17〕 김정숙, 김천식, 윤은준, 홍유식, "RFID와 TCP/IP를 활용한 원격 보안 출입 제어 시스템," 전자공학회논문지, 제45권, 제CI-6호, pp.60-67, 2008.

〔18〕 윤은준, 유기영, "견고한 행렬기반 RFID 상호인증 프로토콜," 한국통신학회논문지, 제33권, 제11호, pp.883-891, 2008.

〔19〕 안해순, 부기동, 윤은준, 남인길, "RFID/USN 환경을 위한 개선된 인증 프로토콜," 전자공학회논문지, 제46권, 제CI-1호, pp.1-10, 2009.

〔20〕 윤은준, 부기동, 하경주, 유기영, "3K-RFID 인증 프로토콜에 대한 공격과 해결책," 한국

통신학회논문지, 제34권, 제6호, pp.578-587, 2009.
〔21〕 윤은준, 유기영, “개선한 일회성 난수를 이용한 RFID 상호인증 프로토콜,” 한국정보과학회논문지, 제36권, 제2호, pp.90-97, 2009.
〔22〕 홍유식, 김천식, 한창평, 오선, 윤은준, “RFID 기술과 신경망 알고리즘을 이용한 불법 주차 차량 감시 방법,” 전자공학회논문지, 제46권, 제CI-4호, pp.13-20, 2009.
〔23〕 Y. Tian, H. Lei, L. Wang, K. Zeng, and T. Fukushima, “A Fast Search Method for Encrypted Medical Data,” Proceedings of the ICC 2009, pp.1-5, 2009.
〔24〕 A. J. Menezes, P. C. Oorschot, and S. A. Vanstone, “Handbook of applied cryptography,” CRC Press, New York, 1997.
[25] B. Schneier, “Applied Cryptography: Protocols, Algorithms and Source Code in C,” 2nd edn. John Wiley, Chichester, 1995.

윤 은 준 (Eun-Jun Yoon) 정회원

1995년 2월 경일대학교 공학사
2003년 2월 경일대학교 컴퓨터공학과 공학석사
2007년 2월 경북대학교 컴퓨터공학과 공학박사
2007년~2008년 대구산업정보대학 컴퓨터정보계열 전임강사
2009년 3월~현재 경북대학교 대학원 전자전기컴퓨터학부 계약교수
<관심분야> 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜

유 기 영 (Kee-Young Yoon) 정회원

1976년 2월 경북대학교 수학과 이학사
1978년 2월 한국 과학 기술원 컴퓨터 공학과 공학석사
1992년 2월 미국 뉴욕 Rensselaer Polytechnic Institute 컴퓨터과학과 이학박사
1978년 3월~현재경북대학교 IT대학 컴퓨터공학부 교수
<관심분야> 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜