RFID 시스템을 위한 안전하고 효율적인 DB 보안 및 인증 기법

정회원 안 해 순*, 종신회원 윤 은 준**, 정회원 부 기 동***, 남 인 길****°

Secure and Efficient DB Security and Authentication Scheme for RFID System

Hae-soon Ahn* *Regular Member*, Eun-jun Yoon** *Lifelong Member*,
Ki-dong Bu***, In-gil Nam****° *Regular Members*

요 약

일반적인 RFID 시스템에서는 백-엔드 데이터베이스 내에 저장되어 있는 대량의 태그 정보들이 암호화되어 있지 않고 평문형태로 저장되어 있다. 이로 인해 외부 해커뿐만 아니라 내부 공격자들에 의해서 태그의 기밀 정보가 쉽게 유출될 수 있다. 만약 태그와 관련된 중요한 정보들이 노출된다면 심각한 프라이버시 침해 문제를 유발시킬 수 있다. 최근 DB 보안에 관한 연구가 중요한 보안 이슈로 대두되고 있음에도 불구하고, RFID 시스템에서의 DB 보안은 전혀 고려되지 않고 있다. RFID 시스템 환경에서 DB 보안 기법을 적용하여 태그 데이터를 암호화하여 백-엔드 데이터베이스 내에 저장한다면 위와 같은 프라이버시 침해와 정보보안 문제를 예방할 수 있다. 따라서 본 논문에서는 RFID 시스템의 백-엔드 데이터베이스에 저장할 태그 식별자와 비밀키를 안전한 DB 비밀키를 사용하여 XOR 연산 기반 암호화 및 복호화하는 안전하고 효율적인 DB 보안 및 인증 기법(S-DB)을 제안한다. 결론적으로 제안한 S-DB 보안 기법은 RFID 시스템 환경의 DB 보안에 적합한 더욱 강력한 보안성과 효율성을 제공할 수 있다.

Key Words : RFID, DB security, Protocol, Mutual authentication, XOR operation, Efficiency

ABSTRACT

In the RFID system, bulk tag information is stored into the back-end database as plaintext format not ciphertext. In this case, the tags's private informations can be easily compromised by an external hacker or an insider attacker. If the private informations of tags disclosed by the attackers, it can occur serious privacy invasion problem. Recently the database(DB) security is an important issue to prevent the above DB compromised attack. However, DB security for RFID systeme has not been considered yet. If we use the DB security technique into the RFID system, the above described privacy invasion problem can be easily prevented. Based on this motivation, this paper proposes a secure and efficient back-end database security and authentication(S-DB) scheme with XOR-based encryption/decryption algorithm. In the proposed scheme, all tag's private information is encrypted and stored by using the DB secret key to protect the DB compromised attack. As a result, the proposed S-DB scheme can provide stronger security and more efficiency for the secure RFID system environment.

* 대구대학교 기초교육원 컴퓨터과정(ahs221@hanmail.net), ** 경북대학교 전자전기컴퓨터학부(ejyoon@knu.ac.kr)
*** 경일대학교 컴퓨터공학과(kdbu@kiu.ac.kr), **** 대구대학교 컴퓨터·IT공학부(ignam@daegu.ac.kr), (° : 교신저자)
논문번호 : KICS2010-12-620, 접수일자 : 2010년 12월 21일, 최종논문접수일자 : 2011년 3월 29일

Ⅰ. 서 론

RFID(Radio Frequency IDentification)는 유비쿼터스 컴퓨팅(ubiquitous computing)의 실현을 위한 매우 중요한 기술 중 하나로 모든 개체에 마이크로 칩을 내장한 태그(tag)를 부착하고, 일정한 주파수 대역을 이용해 무선 통신으로 개체의 정보를 리더(reader)에서 자동으로 인식하고 감지하는 센서 기반 기술이다[1-4]. 또한 단거리 무선 통신(NFC: Near Field Communication) 기술 중에서 정보기술과 자동인식 및 데이터 획득(automatic identification and data capture) 분야에서 빠른 성장세를 보이고 있으며, 출입 통제를 비롯한 출퇴근 관리, 물류 관리 및 주차 관리, 홈 오토메이션 등 산업 분야에서 새로운 대체 기술로서 주목을 받고 있다[5-7].

그러나 무선 통신 채널을 이용하여 인증 절차를 거쳐야 하는 RFID 시스템의 특성으로 인해 상호 인증 과정에서 도청(eavesdropping attack), 스푸핑 공격(spoofing attack), 재전송 공격(replay attack), 서비스 거부 공격(denial of service attack), 위치 트래킹 공격(location tracking attack) 등 악의적인 위협요소들에 쉽게 노출될 수 있는 취약점을 포함하고 있다.

이와 같은 RFID 기술의 취약점들은 개인이나 조직의 보안과 프라이버시 보호에 심각한 문제를 발생시킬 수 있다. 따라서 태그와 리더 그리고 태그의 정보를 저장하고 관리하는 백-엔드 데이터베이스(back-end database) 간에 안전성을 보장할 수 있는 상호 인증 기술이 중요하게 다루어지고 있으며, 최근 들어 RFID 시스템의 보안 취약성을 해결하기 위한 많은 연구가 이루어지고 있다[8-13].

최근에 DB 보안(Database Security)과 관련된 연구가 중요한 보안 이슈로 대두되고 있지만, 실제적으로 RFID 시스템에서는 DB 보안을 심도있게 연구하고 있지 않을 뿐만 아니라 인증 기반의 보안성 개선에 초점을 둔 현실적 RFID 시스템에서는 DB 보안은 많은 관심의 대상이 되지 못하며 깊이 있게 고려되지 않고 있다[14]. 이로 인해 RFID 시스템에서 백-엔드 데이터베이스 내에 저장되어 있는 대량의 태그(tag) 정보들이 암호화 되어 있지 않고 평문(plaintext) 형태로 저장되어 있기 때문에 외부 해커뿐만 아니라 내부 사용자들에 의해서 태그의 기밀 정보 유출을 발생시킬 뿐만 아니라, 태그의 익명성(anonymity) 또한 보장되지 못하고 있다. 만약 태그와 관련된 중요한 정보가 공격자에게 노출된다면 심각한 프라이버시(privacy) 침해와 정보보안 문제를 유발시킬 수 있다. 그러므로 태그와 관련된 기밀 데이터를 암호화하여 백-엔드 데이터베이스 내에 저장한다면 위와 같은 프라이버시 침해와 정보보안 문제를 동시에 예방할 수 있다.

본 논문에서는 위와 같은 RFID 시스템 환경 상에서의 DB 보안의 중요성을 인지하여 RFID 시스템을 위한 안전하고 효율적인 DB 보안 및 인증 기법을 제안한다. 제안한 기법에서는 리더와 백-엔드 데이터베이스 간에 안전하지 않은 통신 채널을 통하여 외부 해커 또는 내부 공격자에 의해 데이터베이스 내의 태그와 관련된 기밀 정보가 유출될 경우를 가정하여, XOR 연산을 기반으로 한 태그들의 식별자와 비밀키를 암호화하여 백-엔드 데이터베이스에 안전하게 저장하고, 암호화된 태그 식별자를 인덱스 검색한 후 해당하는 암호화된 태그 비밀키를 안전하게 복호화하여 인증(authentication)하는 안전하고 효율적인 DB 보안 및 인증(S-DB) 기능을 제공하도록 설계하였다. 결론적으로 제안한 S-DB 보안 기법은 백-엔드 데이터베이스의 태그 식별자와 비밀키를 간단한 XOR 연산을 기반으로 암호화하고, 복호화하기 때문에 강력한 보안성을 제공할 뿐만 아니라 백-엔드 데이터베이스에서의 연산량과 오버헤드를 줄여줌으로써 효율성도 제공한다.

본 논문의 구성은 다음과 같다. II장에서는 관련연구로서 RFID 시스템과 DB 보안에 관해 간단히 설명하고, III장에서는 관련 DB 보안 기술로서 Dawn 등이 제안한 DB 보안 기법에 대하여 검토한다. IV장에서는 제안한 S-DB 보안 프로토콜에 대해 기술하고, V장에서는 보안성 분석, VI장에서는 효율성 분석에 대해 각각 토의한다. 마지막 VII장에서는 본 논문의 결론을 맺는다.

Ⅱ. 관련 연구

본 장에서는 RFID 시스템 구성과 DB 보안의 중요성에 대해 간략하게 살펴본다.

2.1 RFID 시스템 구성

RFID 시스템은 RFID 태그(Tag), RFID 리더(Reader), 백-엔드 데이터베이스(Back-end Database)인 세 가지 컴포넌트로 구성된다[7].

① RFID 태그: RFID 시스템에서 하나의 개체에 부착되어 있는 식별 장치로서, 리더가 질의하면 태그는 자신에게 저장된 식별 정보인 ID를 안전하지 않은 무선 통신 채널을 통해 리더에게 전송한다.

② RFID 리더: RFID 태그와 통신하는 장치로서 리더가 태그에게 질의하여 수집된 정보를 백-엔드 데이

터베이스에게 전송한다. 리더는 소형 단말기 또는 고정된 장치일 수 있다.

③ 백-엔드 데이터베이스: 리더에 의해 읽혀진 태그의 정보는 유·무선 네트워크를 통해 데이터를 처리하는 서버 컴퓨터의 미들웨어로 전달하게 되는데, 이를 일반적으로 백-엔드 데이터베이스라 부른다. 백-엔드 데이터베이스는 처리속도와 저장 공간에 대한 제약을 받지 않는다. 일반적으로 RFID 시스템에서 백-엔드 데이터베이스는 정당한 리더로부터 송신된 임의의 태그에 관한 정보를 수신하고, 이를 이용하여 해당 태그의 정당성을 식별하는 기능을 수행한다.

2.2 DB 보안의 중요성

정보화 사회에서 정보들을 저장하는 저장소인 DB의 관리는 매우 중요한 문제이다. 최근 프라이버시 보호와 정보 보안의 중요성이 크게 대두되면서 DB 보안 문제는 반드시 해결해야 할 시급한 과제가 되었다. DB 보안은 외부 공격자가 발생시키는 프라이버시 침해를 방지할 뿐만 아니라 내부의 DB 관리자나 개발자에 의한 중요 정보 유출까지도 대비하여 개인정보를 보호하는 것을 말한다.

DB에서 관리되는 정보의 양이 급격히 증가됨에 따라 정보의 악용 및 정보 유출은 사회적인 문제로서 그 위험성은 국내뿐만 아니라 전 세계적으로 매우 심각한 상황이다[15]. 유출된 DB의 중요 데이터는 엄청난 금액의 피해와 복구 시간동안 상당한 업무 지장을 초래하게 되고, 무엇보다 가장 큰 문제는 유출된 데이터로 인해 심각한 프라이버시 침해를 유발시킨다는 점이다. 최근 국내에서의 대표적인 DB 정보 유출 사건으로서 옥션 웹사이트 해킹사고 및 하나로 텔레콤의 개인 정보 유출과 관련된 사고의 예를 들어볼 수 있는데, 이로 인해 사회 전반에 걸쳐 개인 정보 보호에 대한 관심이 고조되고 있다. 이러한 DB 보안을 확실하게 보장하는 방법은 정보들을 저장하는 DB의 암호화이다. 만약 암호화된 DB에서 데이터의 일부 또는 백업 받은 DB가 통째로 유출되었다 하더라도 데이터 자체가 암호화되었기 때문에 유출된 중요한 정보는 복호키가 없으면 절대로 복호화할 수가 없다.

이러한 DB 보안 문제는 RFID 시스템 환경에서도 마찬가지이다. 현재 태그의 대량 데이터를 저장 및 관리하고 있는 백-엔드 데이터베이스는 공격자들에 의해 정보의 악용 및 정보 누출은 심각한 사회적 문제로 이슈화되고 있다. RFID 시스템 환경에서의 백-엔드 데이터베이스 정보를 보호하는 방법 역시 태그의 정보를 암호화하여 안전하게 저장하는 것이다.

그러므로 DB 보안과 관련하여 DB를 암호화하고, 암호화된 DB의 효율적이고 실용적인 데이터 검색을 위해 대칭키 암호 기법들을 이용하여 키워드 검색 프로토콜이 제안되었다[16-20]. 특히 Dawn 등[19]에 의해 제안된 DB 보안 관련 기법은 스트림 암호와 블록 암호를 이용하여 키워드 검색을 가능하게 하여 DB 보안과 관련한 대량 데이터에 대한 암호화와 검색에 관한 가장 주목할 만한 선도 연구라 할 수 있다.

Ⅲ. Dawn 등이 제안한 DB 보안 기법

DB 보안과 관련된 연구는 Dawn 등[19]이 XOR 연산을 사용하여 문서 전체를 암호화한 후 DB에 저장하고, 암호화된 문서를 검색하여 복호화하는 기법을 제안 하였다. 이 연구에서는 DB 보안에 대한 기능성과 보안성을 모두 충족할 수 있는 유용한 기법을 제안하였다. 그러나 e-Mail과 같은 텍스트 기반 문서에 대해 순차 탐색과 같은 단순한 검색 알고리즘 상에서 수행하였기 때문에 파일이나 DB처럼 인덱스가 있는 구조적 데이터와, 부울리안, 벡터 혹은 확률 모델 등을 이용한 문서기반의 정보검색 분야에 아직까지는 적용이 어렵다. 본 장에서는 Dawn 등이 제안한 DB 보안 기법을 소개한다. 본 논문에서 사용할 용어들의 표기법 및 정의는 표 1과 같다.

3.1 기본 DB 보안 기법

단어열 $W_1, \ldots, W_l$을 포함하는 문서를 암호화하기 위해 의사난수 비트열과 평문에 대해 XOR 연산을 수행하므로 평문에 관한 어떠한 정보도 노출시키지 않고 원하는 데이터에 대해 안전한 검색이 가능하다. 그림 1은 기본 DB 보안 기법을 보여주고, DB에 저장할

표 1. 용어 정의

기호	의 미
TID	RFID 태그 식별자
DB	백-엔드 데이터베이스(Back-End Database)
k	비밀키
$F()$	안전한 함수(Secure Function)
E	암호 알고리즘
$Query$	검색을 위한 질의어
K_{DB}	백-엔드 데이터베이스의 비밀키
$\|$	연접(concatenation) 연산
$\oplus$	배타적 논리합(XOR; eXclusive OR) 연산

평문에 대한 암호화 과정은 다음과 같다.

Step 1. 평문 W_i는 i번째에 위치해 있는 n 비트 길이의 단어이며, 의사난수 생성기를 사용하여 의사 난수 값들의 열 $S_1, ..., S_j$을 생성한다.

Step 2. S_i는 i번째에 위치해 있는 $n-m$ 비트이고, i번째에 위치해 있는 n 비트 길이의 단어 W_i를 암호화하기 위해 의사난수 비트열 S_i와 키 값 k_i를 가지고 $F_{ki}(S_i)$를 구한다.

Step 3. 암호문 $C_i = W_i \oplus (S_i \| F_{ki}(S_i))$를 생성한다. 만약 어떤 단어에 대한 검색을 하고자 한다면, 검색할 단어 W와 W가 위치할 만한 i번째 위치에 해당하는 키 k_i를 DB에게 말해주면, DB는 $C_i \oplus W_i$가 $(S_i \| F_{ki}(S))$의 형태인지를 확인하고, 암호문을 검색한다. 그러나 이 기본 DB 보안 기법에서 단어 검색을 하려면 사전에 그 단어가 위치해 있는 키 값을 알아야하거나 모든 키 값 k_i를 공개해야 하기 때문에 효율적인 검색에 적합한 편은 아니다.

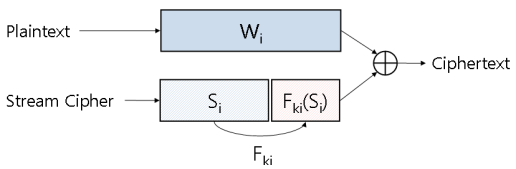

그림 1. 기본 DB 보안 기법

3.2 은닉 쿼리 기반 DB 보안 기법

단어 W에 대한 검색을 요청하고자 할 때 단어 W에 대해 어떠한 정보도 노출시키고 싶지 않다면 쿼리를 암호화하면 된다. 그림 2는 은닉 쿼리 기반 DB 보안 기법을 보여준다.

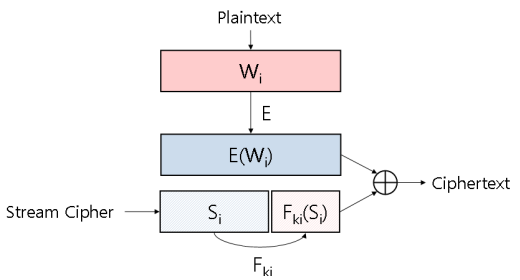

그림 2. 은닉 쿼리 기반 DB 보안 기법

Step 1. 전체 문서의 각 단어들을 암호 알고리즘 E를 사용하여 사전에 암호화시킨다. 이때, 사전 암호화 단계에서는 블록 암호를 사용하여 문서의 단어들을 암호화하고, 암호화된 단어열이 생성된다.

Step 2. 의사난수 생성기를 사용하여 의사 난수 값들의 열 $S_1, ..., S_j$을 생성한다.

Step 3. S_i는 i번째에 위치해 있는 $n-m$ 비트이고, i번째에 위치해 있는 n 비트 길이의 사전 암호화된 $E(W_i)$ 단어열을 다시 암호화하기 위해 의사난수 비트열 S_i와 키 값 k_i를 가지고 $F_{ki}(S_i)$를 구한다.

Step 4. 암호문 $C_i = E(W_i) \oplus (S_i \| F_{ki}(S_i))$를 생성한다. 이때, 단어 W를 검색하기 위해 $Query(E(W_i))$를 DB에게 보내게 된다. 따라서 사전에 암호화하는 E가 안전하다면 단어 W를 노출시키지 않고 검색할 수 있도록 함으로써 은닉 쿼리 검색이 가능한 DB 보안 기법이 된다.

Ⅳ. 제안한 S-DB 보안 기법

앞 장에서 Dawn 등[19]에 의해 제안된 대량 데이터에 대한 암호화와 검색에 관한 연구를 간단히 검토해 보았다. 본 논문에서는 XOR 연산을 통해 암호화와 복호화를 시도한 Dawn 등의 연구를 기반으로 RFID 시스템 환경에 적용 가능한 S-DB 보안 기법을 제안한다. 기존 RFID 상호 인증 프로토콜 연구들에서는 RFID 시스템 환경에서의 리더와 백-엔드 데이터베이스와의 통신은 안전한 채널임을 가정하였다[21-24]. 그러나 실제로는 리더와 백-엔드 데이터베이스 간의 통신 채널도 안전하지 않으며, 비록 안전하다 할지라도 백-엔드 데이터베이스에 저장되어 있는 태그 정보들이 암호화 되어 있지 않고 평문으로 저장되어 있기 때문에 외부 해커뿐만 아니라 내부 사용자들에 의해서도 태그의 정보가 유출될 수 있다. 만약 개인 정보나 중요한 자료가 노출된다면 심각한 프라이버시 침해와 정보보안 문제를 유발시킨다. 그러므로 태그 데이터 자체를 암호화하여 백-엔드 데이터베이스에 저장 및 관리한다면 프라이버시와 개인정보 보호를 더욱 강화시킬 수 있다. 본 장에서는 RFID 시스템 환경에서 백-엔드 데이터베이스에 저장할 태그 식별자와 비밀키에 관한 정보를 암호화하고, 복호화하는 S-DB 보안 기법에 대해 설명한다.

4.1 DB 내의 태그 비밀키 암호화

모든 태그의 식별자 TID와 비밀키 k_{TID}는 고정된 길이 단어의 m 비트열이며, K_{DB}는 백-엔드 데이터베이스의 비밀키이다. 그리고 $F_{K_{DB}}(\cdot)$는 K_{DB}를 이용한 메시지 인증 코드(MAC)이다. 그림 3은 태그 비밀키 암호화 기법이며, 과정은 다음과 같다.

Step 1. 태그의 TID와 백-엔드 데이터베이스의 비밀키 K_{DB}를 이용하여 고유한 MAC 값인 m 비트열 길이의 $F_{K_{DB}}(TID)$ 값을 계산한다.

Step 2. m 비트열 길이의 태그 TID의 비밀키 k_{TID}와 위에서 구한 $F_{K_{DB}}(TID)$를 $k_{TID} \oplus F_{K_{DB}}(TID)$의 비트 단위 XOR 연산을 수행하여 암호화된 태그 비밀키 값인 $C_{TID} = k_{TID} \oplus F_{K_{DB}}(TID)$를 계산한다.

Step 3. $C_{TID} = k_{TID} \oplus F_{K_{DB}}(TID)$인 암호화 된 태그 비밀키 값을 해당 태그의 비밀키 필드 내에 저장한다.

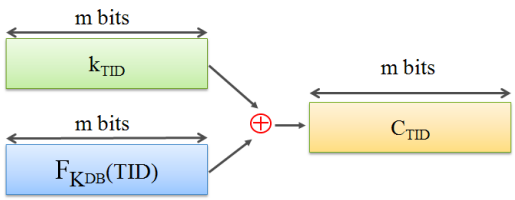

그림 3. DB 내의 태그 비밀키 암호화

4.2 DB 내의 태그 비밀키 복호화

그림 4는 DB 내의 태그 비밀키 복호화 기법을 보여준다. 리더로부터 임의의 태그에 대한 인증 요청 메시지를 수신하였다고 가정하자. 그러면 DB는 다음의 과정을 수행하여 안전하게 태그 인증을 수행할 수 있다.

Step 1. $C_{TID} = k_{TID} \oplus F_{K_{DB}}(TID)$인 암호화된 태그 비밀키 값을 해당 태그의 비밀키 필드로부터 읽어온다.

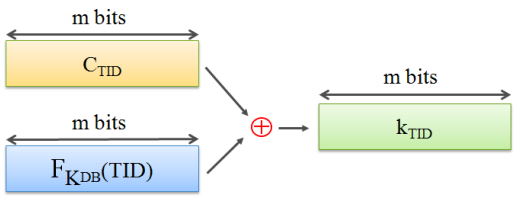

그림 4. DB 내의 태그 비밀키 복호화

Step 2. 태그의 TID와 백-엔드 데이터베이스의 비밀키 K_{DB}를 이용하여 고유한 MAC 값인 m 비트열 길이의 $F_{K_{DB}}(TID)$ 값을 계산한다.

Step 3. 위에서 각각 구한 C_{TID}와 $F_{K_{DB}}(TID)$를 $C_{TID} \oplus F_{K_{DB}}(TID)$의 비트 단위 XOR 연산을 수행하여 태그의 비밀키 k_{TID}를 얻는다. 여기에서 C_{TID}는 $k_{TID} \oplus F_{K_{DB}}(TID)$이므로 $C_{TID} \oplus F_{K_{DB}}(TID)$ 연산의 결과는 아래와 같이 k_{TID}가 됨을 쉽게 알 수 있다.

$$\begin{aligned} & C_{TID} \oplus F_{K_{DB}}(TID) \\ &= k_{TID} \oplus F_{K_{DB}}(TID) \oplus F_{K_{DB}}(TID) \\ &= k_{TID} \end{aligned}$$

Step 4. DB는 복호화하여 얻은 k_{TID}를 이용하여 리더로부터 수신한 메시지의 합법성 검증을 통하여 태그를 인증할 수 있다.

4.3 DB 내의 태그 식별자 암호화

그림 5는 DB 내의 태그 식별자 암호화 기법이며, 과정은 다음과 같다.

Step 1. 태그의 TID와 백-엔드 데이터베이스의 비밀키 K_{DB}를 이용하여 고유한 MAC 값인 m 비트열 길이의 $F_{K_{DB}}(TID)$ 값을 계산한다.

Step 2. m 비트열 길이의 태그 식별자 TID와 위에서 구한 $F_{K_{DB}}(TID)$를 $TID \oplus F_{K_{DB}}(TID)$의 비트 단위 XOR 연산을 수행하여 암호화된 태그 식별자 값인 $X_{TID} = TID \oplus F_{K_{DB}}(TID)$를 계산한다.

Step 3. $X_{TID} = TID \oplus F_{K_{DB}}(TID)$인 암호화된 태그 식별자 값을 해당 태그의 식별자 필드 내에 저장한다.

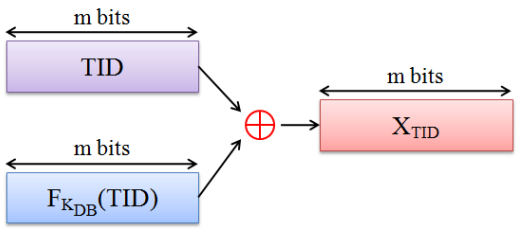

그림 5. DB 내의 태그 식별자 암호화

4.4 DB 내의 태그 식별자 복호화

그림 6은 DB 내의 태그 식별자 복호화 기법이며,

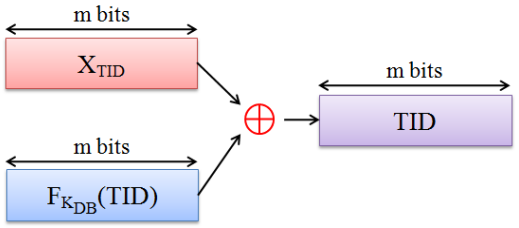

그림 6. DB 내의 태그 식별자 복호화

과정은 다음과 같다.

Step 1. $X_{TID} = TID \oplus F_{K_{DB}}(TID)$인 암호화된 태그 식별자 값을 해당 태그의 식별자 필드로부터 읽어온다.

Step 2. 태그 식별자 TID와 백-엔드 데이터베이스의 비밀키 K_{DB}를 이용하여 고유한 MAC 값인 m 비트열 길이의 $F_{K_{DB}}(TID)$ 값을 계산한다.

Step 3. 위에서 각각 구한 X_{TID}와 $F_{K_{DB}}(TID)$를 $X_{TID} \oplus F_{K_{DB}}(TID)$의 비트 단위 XOR 연산을 수행하여 태그 식별자 TID를 얻는다. 여기에서 X_{TID}는 $TID \oplus F_{K_{DB}}(TID)$이므로 $X_{TID} \oplus F_{K_{DB}}(TID)$ 연산의 결과는 아래와 같이 TID가 됨을 쉽게 알 수 있다.

$$\begin{aligned} & X_{TID} \oplus F_{K_{DB}}(TID) \\ &= TID \oplus F_{K_{DB}}(TID) \oplus F_{K_{DB}}(TID) \\ &= TID \end{aligned}$$

Step 4. DB는 복호화하여 얻은 TID를 이용하여 리더로부터 수신한 메시지의 합법성 검증을 통하여 태그를 인증할 수 있다.

백-엔드 데이터베이스내의 태그 식별자와 암호화된 비밀키 및 그 외 태그들의 정보가 저장된 형태는 표 2와 같다.

$$X_{TID_i} = TID_i \oplus F_{K_{DB}}(TID_i)$$
$$C_{TID_i} = k_{TID_i} \oplus F_{K_{DB}}(TID_i)$$

표 2. 백-엔드 데이터베이스내의 태그 저장 형태

인덱스	암호화된 태그 식별자	암호화된 태그 비밀키	태그 정보
1	X_{TID_1}	C_{TID_1}	Info1
2	X_{TID_2}	C_{TID_2}	Info2
3	X_{TID_3}	C_{TID_3}	Info3
...	...	...	...
n	X_{TID_n}	C_{TID_n}	Infon

V. 보안성 분석

본 장에서는 제안한 S-DB 보안 기법의 안전성에 대해 분석한다. 먼저 제안한 S-DB 보안 기법의 분석에서 필요로 하는 안전성은 다음과 같이 정의 및 가정된다.

[가정 1]. DB의 강력한 비밀 키(K_{DB})는 다항식 시간 안에 추측될 수 없는 높은 엔트로피 $S(K)$ 값이다.

[가정 2]. 안전한 메시지 인증 코드 함수 $y = F(x)$에서 주어진 x로 y를 계산하는 것은 쉽고, 주어진 y로 x를 계산하는 것은 어렵다.

위에서 정의된 것을 고려하여 다음과 같은 이론들이 제안한 S-DB 보안 기법의 안전성 분석에 사용된다.

[정리 1]. 제안한 S-DB 보안 기법은 임의의 공격자에 의한 백-엔드 데이터베이스 유출 공격에 안전하다.

[증명 1]. 먼저 모든 태그들의 비밀키 정보를 저장하고 있는 백-엔드 데이터베이스 내의 태그 관리 테이블이 유출되었다고 가정하자. 기존의 RFID 시스템에서는 이러한 백-엔드 데이터베이스 유출로 인해 임의의 공격자는 암호화되어 있지 않는 백-엔드 데이터베이스 테이블로 부터 간단히 모든 태그들의 비밀키 k_{TID}를 쉽게 얻을 수 있다. 하지만 제안한 S-DB 보안 기법 상에서는 공격자가 태그의 비밀키 정보를 담고 있는 백-엔드 데이터베이스 테이블의 값들을 획득하더라도 해당 태그의 비밀키 k_{TID}가 아닌 암호화된 $C_{TID} = k_{TID} \oplus F_{K_{DB}}(TID)$를 얻게 된다. 따라서 DB의 비밀키인 K_{DB}로 암호화된 $C_{TID} = k_{TID} \oplus F_{K_{DB}}(TID)$는 DB의 비밀키인 K_{DB}를 모르고서는 C_{TID}로 부터 태그의 비밀키 k_{TID}를 복호화할 수 없다. 결론적으로 제안한 S-DB 보안 기법은 임의의 공격자에 의한 백-엔드 데이터베이스 유출 공격에 안전하다.

[정리 2]. 제안한 S-DB 보안 기법은 합법적인 임의의 태그에 의한 백-엔드 데이터베이스 유출 공격에 안전하다.

[증명 2]. 만약 합법적인 한 태그의 비밀키 k_{TID}를 알고 있는 공격자라 하더라도 $C_{TID} = k_{TID} \oplus F_{K_{DB}}(TID)$로부터 $C_{TID} \oplus k_{TID}$를 계산하여 $F_{K_{DB}}(TID)$

를 얻을 수는 있지만, 위 [정의 1]과 [정의 2]에 의해 백-엔드 데이터베이스의 비밀키인 K_{DB}는 여전히 얻을 수 없음으로 나머지 태그들의 비밀키 안전성을 보장할 수 있다. 결론적으로 제안한 S-DB 보안 기법은 합법적인 임의의 태그에 의한 백-엔드 데이터베이스 유출 공격에 대해 안전하다.

[정리 3]. 제안한 S-DB 보안 기법은 태그 식별자(TID)가 백-엔드 데이터베이스 내에 암호화하여 저장되어 있으므로 백-엔드 데이터베이스 유출 공격에 안전하다.

[증명 3]. 태그 식별자는 RFID 시스템에서 상호 인증을 위해 리더와 태그 또는 DB와 리더 간에 전송될 수 있다. 이때 전송되는 태그 식별자 TID는 요청 값으로서 바로 전송되거나 안전한 일방향 해쉬 함수에 의해 은닉 질의로 전송되는 다음과 같은 두 가지 경우가 존재할 수 있다.

Case 1: 인증 과정에서 태그 식별자 값인 TID가 전송될 경우 공격자는 TID를 가로챌 수 있다. 비록 공격자가 태그 식별자 TID를 알고 있더라도 백-엔드 데이터베이스에는 해당 태그의 식별자 TID가 아닌 암호화된 태그 식별자 값 $X_{TID} = TID \oplus F_{K_{DB}}(TID)$를 얻게 된다. 따라서 DB의 비밀키인 K_{DB}로 암호화된 $X_{TID} = TID \; F_{K_{DB}}(TID)$는 DB의 비밀키인 K_{DB}를 모르고서는 태그 식별자 TID를 암호화할 수 없을 뿐만 아니라 백-엔드 데이터베이스에 저장되어 있는 X_{TID}로 부터 태그의 식별자를 복호화할 수 없다. 결론적으로 제안한 S-DB 보안 기법은 임의의 태그 식별자 TID를 가로챈 공격자에 의한 백-엔드 데이터베이스 유출 공격에 안전하다.

Case 2 : RFID 시스템의 인증 과정에서 태그 식별자 TID가 일방향 해쉬 함수로 은닉한 값 $h(TID)$로 전송될 경우 공격자가 가로챌 수 있다. 그러나 이 경우에도 백-엔드 데이터베이스에는 DB의 비밀키인 K_{DB}로 암호화된 태그 식별자 $X_{TID} = TID \; F_{K_{DB}}(TID)$가 저장되어 있으므로 DB의 비밀키인 K_{DB}를 모르고서는 태그 식별자 TID를 암호화할 수 없을 뿐만 아니라 DB에 암호화되어 저장되어 있는 X_{TID}로 부터 태그의 식별자를 복호화할 수 없다. 결론적으로 제안한 S-DB 보안 기법은 임의의 태그 식별자가 일방향 해쉬 함수로 은닉한 값 $h(TID)$를 가로챈 공격자에 의한 백-엔드 데이터베이스 유출 공격에 안전하다.

Ⅵ. 효율성 분석

본 논문에서 제안한 S-DB 보안 기법은 간단한 비트 단위 XOR 연산을 기반으로 설계하였다. 표 3은 은닉쿼리 기반 DB 보안 기법과 비교하여 제안한 S-DB 보안 기법에서 백-엔드 데이터베이스에 저장되어 있는 태그 식별자와 비밀키를 암호화와 복호화할 때 사용한 연산량을 비교 및 계산한 표이다.

RFID 환경에 사용되어 질 수 있는 기존의 은닉 쿼리 기반 DB 보안 기법은 대칭키 암호 알고리즘을 기반으로 복잡한 연산들을 수행하여 DB 내의 데이터를 암호화하므로 데이터 검색시 복호화할 때 연산 오버헤드 뿐만 아니라 비용면에서도 효율적이지 못하다. 그러나 제안한 S-DB 보안 기법에서는 백-엔드 데이터베이스 내의 태그 식별자와 비밀키 암호화 연산으로 XOR과 해쉬 연산을 각각 한 번씩만 수행하면 되므로 n개의 태그에 대해 n번의 XOR과 해쉬 연산이 요구된다. 그리고 검색시 복호화할 경우 우선 n개의 태그 식별자에 대해 n번의 복호화 연산이 수행된 후 해당 태그 식별자에 대해서는 1번의 태그 비밀키 복호화 연산만이 요구된다.

따라서 S-DB 보안 기법은 기존 DB 보안 기법보다 많은 연산량을 줄이고 안전성과 효율성을 제공한다. 무엇보다 Dawn 등이 제안한 DB 보안 기법은 유비쿼터스 컴퓨팅 환경 기반에서의 RFID 시스템 DB 보안

표 3. 제안한 S-DB 기법과 은닉쿼리 기반 DB 보안 기법과의 연산량 비교

	은닉쿼리 기반 DB 보안 기법		제안한 S-DB 보안 기법			
	평문 암호화	평문 복호화	태그 식별자 암호화	태그 식별자 복호화	태그 비밀키 암호화	태그 비밀키 복호화
대칭키 연산	n	n	n	n	n	1
해쉬 연산	n	n	n	n	n	1
XOR 연산	n	n	n	n	n	1

n : 백-엔드 데이터베이스에 저장된 태그 수

기법으로는 적합하지 않다. 왜냐하면 백-엔드 데이터베이스에 데이터를 암호화하여 저장하기에는 태그 수가 너무 많고, RFID 태그의 제한된 자원과 저전력 통신환경에서는 대칭키 기반 암호화기법은 비효율적이기 때문이다. 결론적으로 제안한 S-DB 보안 기법은 기존의 방법들보다 더욱 효율적인 검색 기법을 제공할 수 있다.

Ⅶ. 결론 및 향후연구

본 논문에서는, RFID 시스템에서 백-엔드 데이터베이스 내에 대량의 태그 데이터를 암호화하기 위해 XOR 연산을 기반으로 한 암호 기법을 이용하여 태그들의 식별자와 비밀키를 암호화하여 저장하고, 암호화된 태그 식별자를 검색한 후 복호화하고, 해당 태그의 암호화된 비밀키를 복호화하는 기법인 S-DB 보안 기법을 제안하였다. 이 S-DB 보안 기법은 백-엔드 데이터베이스의 데이터 자체를 DB 비밀키로 암호화하기 때문에 정보보호를 더욱 강화시키고, XOR 연산 기반 암호 기법이므로 검색시 백-엔드 데이터베이스에서의 연산량과 오버헤드를 줄여줌으로써 연산 비용이 실용가능한 수준에서 이루어질 수 있게 하였다.

향후 연구는 백-엔드 데이터베이스에 저장되어 있는 암호화된 데이터에 대한 질의와 복호화를 통한 인덱스 검색 기능을 확장하여 태그 정보 데이터에 적용함으로써 더욱 강화된 DB 보안 기능을 갖는 기법을 구현하는 것이다.

참 고 문 헌

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

〔2〕 S. Shepard, "RFID: Radio Frequency Identification", New York, USA: Mc Graw Hill, 2005.

〔3〕 L. Srivastava, "Ubiquitous network societies: The case of Radio Frequency Identification, background paper", International telecommunication union (ITU) new initiatives workshop on ubiquitous network societies, Geneva, Switzerland, 2005.

〔4〕 B. Glover and H. Bhatt. RFID Essentials. O'Reilly, 2006

〔5〕 D. Lin, H. G. Elmongui, E. Bertino, and B. C. Ooi, "Data management in RFID applications", International conference on database and expert systems applications, Vol.4653 of LNCS, pp.434-444, 2007.

〔6〕 M. Lehtonen, T. Staake, F. Michahelles, and E. Fleisch. From identification to authentication - a review of RFID product authentication techniques. In Printed handout of Workshop on RFID Security (RFIDSec 2006).

〔7〕 K. Finkenzeller, "RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification", (2nd ed.), Munich, Germany: Wiley, 2003.

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

〔9〕 S. Weis, S. Sarma, R. Rivest, and D. Engels. "Security and privacy Aspects of Low-Cost Radio Frequency Identification Systems", In D. Hutter, G. M¨uller, W. Stephan, and M. Ullmann, editors, International Conference on Security in Pervasive Computing (SPC 2003), Vol.2802 of LNCS, pp.454-469, 2003.

〔10〕 S. S. Yeo and S. K. Kim, "Scalable and Flexible Privacy Protection Scheme for RFID System", In Proceedings of the 2nd European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS 2005), Vol.3813 of LNCS, pp.153-163, July 2005.

〔11〕 D. Molnar and D. Wagner, ″Privacy and security in library RFID: issues, practices, and architectures″, Conference on Computer and Communications Security-CCS'04, pp.210-219, 2004.

〔12〕 S. S. Yeo, K. Sakurai, S. E. Choi, K. S. Yang, and S. K. Kim, "Forward Secure Privacy Protection Scheme for RFID System Using Advanced Encryption Standard", In Proceedings of Frontiers of High Performance Computing and Networking ISPA 2007 Workshops, Vol.4743 of LNCS, pp.245-254, 2007.

〔13〕 이근우, 오동규, 곽진, 오수현, 김승주, 원동호, "분산 데이타베이스 환경에 적합한 Challenge-Response 기반의 안전한 RFID 인증 프로토콜," 한국정보처리학회 논문지C, 제12-C권, 제03호,

pp.309-316, 2005.
〔14〕 윤은준, 유기영, “의료정보보호를 위한 RFID를 이용한 환자 인증 시스템,” 한국통신학회논문지, 제35권, 제6호, pp.962-969, 2010.
〔15〕 A. Gordon, M. P. Loeb, W. Lucyshyn, and R. Richardson, “2004 CSI/FBI Computer Crime and Security Survey”, Ninth annual report of computer security society, CSI, 2004. For general information, refer to “http://gocsi.com or http://www.nipc.gov”
〔16〕 Y. Chang and M. Mitzenmacher, “Privacy preserving keyword searches on remote encrypted data”, In Proceedings of ACNS‘05, Vol.3531 of LNCS, pp.442-445, 2005.
〔17〕 D. J. Park, K. Kim, and P. J. Lee, “Public Key Encryption with Conjunctive Field Keyword Search”, In Proceedings of WISA’04, Vol.3325 of LNCS, pp.73-86, 2004.
〔18〕 P. Golle, J. Staddon, and B. Waters, “Secure Conjunctive Keyword Search Over Encrypted Data”, In Proceedings of ACNS’04, Vol.3089 of LNCS, pp.31-45, Springer-Verlag, 2004.
〔19〕 X. Dawn, D. Wagner and A. Perrig, ″Practical Techniques for Searches on Encrypted Data″, Proceedings of the 2000 IEEE Symposium on Security and Privacy, p.44, 2000.
〔20〕 변진욱, “암호화 문서상에서 효율적인 키워드 검색 프로토콜 설계,” 전자공학회논문지, 제46권, 제CI-1호, pp.46-55, 2009.
〔21〕 안해순, 부기동, 윤은준, 남인길, “TRMA: 2-라운드 RFID 상호 인증 프로토콜,” 전자공학회논문지, 제46권, 제CI-5호, pp.71-78, 2009.
〔22〕 안해순, 부기동, 윤은준, 남인길, “RFID/USN 환경을 위한 개선된 인증 프로토콜,” 전자공학회논문지, 제46권, 제CI-1호, pp.1-10, 2009.
〔23〕 전서관, 은선기, 우수현, “상호인증을 제공하는 개선된 RFID 인증 프로토콜,” 전자공학회논문지, 제47권, 제TC-2호, pp.113-120, 2010.
〔24〕 김정숙, 김천식, 윤은준, 홍유식, “RFID와 TCP/IP를 활용한 원격 보안 출입 제어 시스템,” 전자공학회논문지, 제45권, 제CI-6호, pp.60-67, 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, 정보검색, 데이터베이스 보안, RFID 보안

윤 은 준 (Eun-Jun Yoon) 종신회원

2003년 경일대학교 컴퓨터공학과(공학석사)
2007년 경북대학교 컴퓨터공학과(공학박사)
2007년~2008년 대구산업정보대학 컴퓨터정보계열 전임강사
2008년~현재 경북대학교 전자전기컴퓨터학부 BK21 계약교수
<관심분야> 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜

부 기 동 (Ki-Dong Bu) 정회원

1984년 경북대학교 전자공학과(공학사)
1988년 경북대학교 전자공학과(공학석사)
1996년 경북대학교 전자공학과(공학박사)
1983년~1985년 포항종합제철 시스템개발실
2001년~2002년 일본 게이오대학 방문교수
1988년~현재 경일대학교 컴퓨터공학과 교수
<관심분야> 데이터베이스, GIS, 시멘틱 웹, 데이터베이스 보안, RFID 보안

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