NFC 기반 환자 인증 시스템 설계

정규환*, 박석천**

*가천대학교 일반대학원 모바일 소프트웨어학과
**가천대학교 컴퓨터공학과 정교수(교신저자)

e-mail : davius@hanmail.net

The NFC-based Patient Authentication System Design

Kyu-Hwan Jung*, Seok-Cheon Park**

*Dept. of Mobile Software, Gachon University
**Dept. of Computer Engineering, Gachon University

요 약

오늘날 의료 사고 방지를 대책으로 RFID/NFC 와 같은 근접 무선 통신 기술을 적용의 사례가 많아 지고 있는 가운데 현재 RF 스마트 카드를 이용한 환자 인증 시스템 도입으로 인해 의료 정보의 정확성과 효율성을 높여 주고 있다. 하지만, RFID(Radio Frequency IDentification)의 기술적 보안 취약점이 발견됨에 따라 이에 대안으로 본 논문에서는 보안성이 뛰어난 NFC(Near Field Communication) 기반 환자 인증 시스템을 제안하고자 한다.

1. 서론

현재 우리는 정보 기술(IT)과 초고속 통신망의 발달로 언제 어디서나 정보를 쉽게 접할 수 있는 환경의 Ubiquitous 시대에 살고 있다. 의료 분야에서도 정보기술과 네트워크를 융합하여 '언제나, 어디서나' 이용 가능한 건강관리 및 의료 서비스를 지칭하는 u-Health 산업이 등장하여 병원 정보 시스템 선진화와 다양한 의료 서비스 모델에 대한 개발 및 연구가 활발하게 이루어지고 있다. 특히 불필요한 수술, 잘못된 약물 처방, 또는 약물 이상 반응 등과 같은 의료 과실을 줄이기 위한 방법으로 RFID(Radio Frequency IDentification)와 같은 근거리 무선 통신기술을 많이 적용하고 있다. 최근에는 NFC(Near Field Communication)와 같은 근거리 무선 통신기술이 스마트 폰에 적용되어 근거리 무선 통신 기술의 보급과 활용도가 점점 높아지고 있다. 이와 같이 RFID, NFC 와 같은 근접 무선 통신 기술은 Ubiquitous 환경 실현을 위한 중요한 핵심 기술로 가장 주목을 받고 있는 기술이다[1].

현재 병원에서 사용되고 있는 환자 인증 시스템은 RF 스마트 카드를 이용한 환자 인증 시스템을 사용하고 있는데, RFID 태그는 태그 자체의 연산 능력이 떨어지며, 객체를 유일하게 식별하기 위한 최소한의 정보만을 가지며, 정보 노출, 위치 추적 등으로 개인의 프라이버시 침해를 유발할 수 있는 문제점을 지니고 있다. 따라서 의료 환경에서 근접 무선 통신 기술 활용을 위해 반드시 고려되어야 할 핵심은 프라이버시 제공 여부이다[1].

본 논문에서는 위와 같은 의료 환경을 기반으로 안전하고 효율적으로 환자 인증 및 환자 개인 정보를 보호할 수 있는 NFC 환자 인증 시스템을 제안한다. 제안하는 NFC 환자 인증 시스템은 강인한 보안성과 효율성을 제공해 주어, 첨단 의료 환경에서 환자 개인의 프라이버시 제공 및 정보보호를 위해 실용적으로 사용되어 질 수 있다.

본 논문의 구성은 다음과 같다. 2 장에서는 NFC 기술에 대한 개요와 보안 취약점을 강화 하기 위한 NFC 보안 기술에 대해 논하고, 3 장에서는 기존의 RFID 환자 인증 시스템에 대한 설명과 취약점을 살펴보고, 4 장에서는 본 논문에서 제안하는 NFC 환자 인증 시스템 설계를 기술하고 최종적으로 5 장에서 결론 및 향후 연구로 끝을 맺는다.

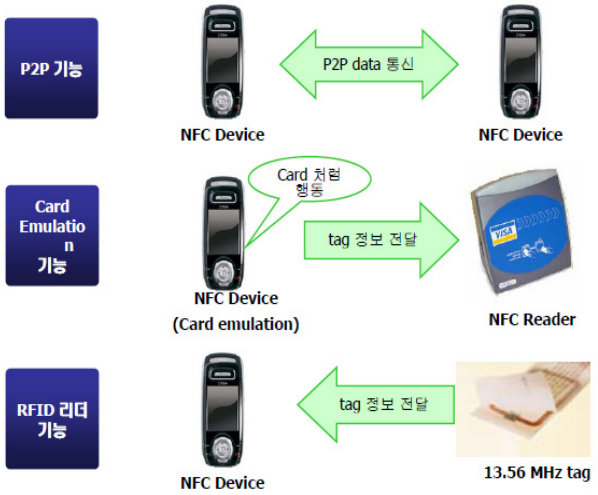
2. 관련 연구

2.1 NFC 기술 개요

NFC 는 13.56MHz 대역의 통신 주파수에서 106kbps 에서 424Kbps 의 통신 속도를 제공하며 통신 범위가 약 10cm 이내인 초 근접거리 무선 통신 기술이다. NFC 는 네트워크 설정에 필요한 시간이 0.1 초 수준으로, 타 근접 문선 통신 기술과 차별화된 즉시 응답성이 필요한 형태의 응용에 매우 적합한 기술이다.

NFC 는 두 단말의 안테나를 통하여 유도기 전력을 기반으로 통신하는 기술로 각 단말의 전자기장의 생

성 여부에 따라 수동 통신(passive communication)모드와 능동 통신(active communication)모드로 동작한다. 능동 통신 모드는 단말이 캐리어 주파수에 전자기장을 생성하여 다른 단말에 유도기 전력을 공급하여 통신을 수행하는 모드로 일반적으로 전원이 필요한 모드이다. 수동 통신 모드는 단말이 스스로 전자기장을 생성하지 않고, 능동 통신 모드의 단말이 생성한 전자기장으로부터 유도되는 전력을 이용하여 통신을 수행하는 모드를 말한다. 이러한 2 개 모드를 활용하면 NFC 단말은 다음 그림 1 과 같은 3 가지 형태의 동작 모드로 통신을 수행할 수 있다.



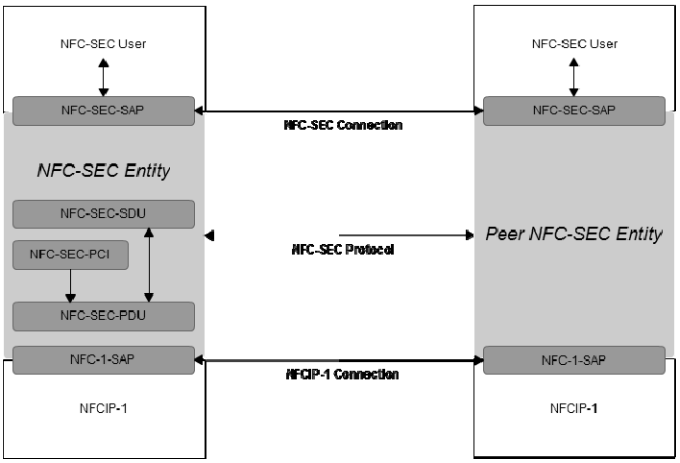
(그림 1) NFC 동작 모드

- 카드 모드: NFC 단말의 수동 통신 모드 동작으로, RFID 태그처럼 내부 전원 없이 외부의 리더기/기록기에 NFC 카드의 정보를 제공하여, 기존 RFID 의 응용을 지원할 수 있다. 이 모드는 ISO/IEC 14443 의 표준을 준수하여 기존 스마트 카드에서 사용하던 모바일 결제 서비스 등을 사용할 수 있으며, 그 외에 출입통제, 교통카드 등의 응용에 사용 가능하다.
- RFID 리더기/기록기 모드 : NFC 단말의 능동 통신 모드의 동작으로 외부의 수동 통신 모드 NFC 및 RFID 의 정보를 읽거나, 전자지갑에서 이용 요금을 지불하는 등의 응용에 주로 사용되며, 기존 RFID 를 활용하여 사용자에게 제공하여 못하던 새로운 응용을 제공할 수 있다.
- 동등 계층 통신 모드(pear to pear) : 두 단말이 모두 능동 통신 모드로 통신하여 두 단말의 각자의 전자기장을 생성하여 상호 통신을 수행하는 모드이다. 이 모드를 활용하면 스마트 기기 간 정보를 능동적으로 상호간 송수신 할 수 있어 명함 교환이나, 사진, 동영상, 등의 교환이 가능하며, 전자 지갑의 일환으로 동등 계층간 자금 이체 등이 가능하다.

NFC 는 RFID 의 리더기/기록기 모드로의 동작과 동등계층 통신의 지원으로 기존 RFID 에서 제공하지 못하던 새로운 응용을 제공하거나, 기존 RFID 에서 가지고 있던 보안상의 이슈를 해소하는 등의 이점을 얻을 수 있다. 이러한 특징을 활용하여 안전하고 편리하고 다양한 상황에서 사용 가능한 범용적 인증 방식을 도입하면 다양한 응용에서 NFC 모바일 기기를 통해 해당 서비스를 활용할 수 있도록 지원 가능해진다[3].

2.2 NFC 보안 기술

NFC 보안 기술은 NFC Forum 을 중심으로 ECMA 표준을 기반으로 데이터 교환 형식 및 태그 타입, 보안 프로토콜에 대해 정의하고 있다. NFC 보안 관련 주요 표준은 ECMA 에서 발표한 ECMA-385 에 있으며 주 내용은 NFCIP-1 데이터 교환을 위한 보안 서비스 및 보안 프로토콜을 제시하고 있다. ECMA-385 는 NFCIP-1 에 의해 NFC 기기 간의 통신이 연결 된 후 보안 서비스를 수행하고, NFC-SEC-SAP 를 통해 NFC-SEC 서비스에 접근한다. NFC-SEC 서비스는 NFC-SEC 프로토콜로 NFC-SEC-PDU 를 교환한다. 다음 그림 2 는 NFC-SEC 의 보안 계층 구조과 보안 프로토콜을 나타낸다[6].



(그림 2) NFC-SEC 의 보안 계층 구조

NFC-SEC 에서는 SSE 와 SCH 보안 서비스를 제공한다[6].

2.2.1 보안 서비스

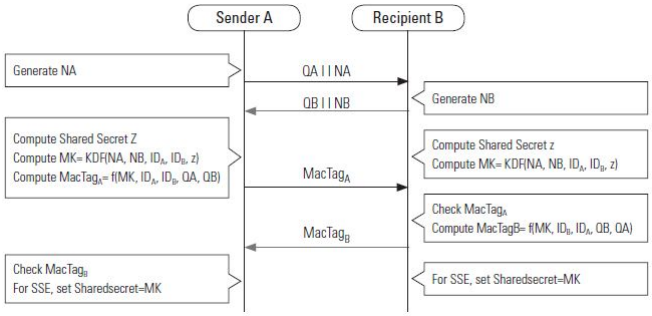
- SSE(Shared Secret Service)
  NFC 디바이스간의 암호통신을 위한 공유 비밀을 생성하며, 이 과정에서 키 일치 및 확립 과정을 수행한다.

- SCH(Secure Channel Service)
  SSE 서비스를 통해 생성된 링크키를 통해 NFC 디바이스간의 통신 데이터에 대한 기밀성과 무결성을 제공한다.

또한 ECMA 는 NFC-SEC 의 보안 구조 하에 보안 매커니즘인 ECMA-386(NFC-SEC-01)을 제시하였다.

2.2.2 보안 매커니즘

우선 모바일 NFC 기기는 EC(Elliptic Curve Diffie-Hellman) 공개 키와 개인 키를 소유한다는 가정 하에 SSE 와 SCH 를 시행한다. 그림 3 은 SSE 를 위해 키(MK) 공유 과정을 나타내며 다음은 각 과정에 대한 설명이다[6].



(그림 3) ECMA-386

① Elliptic Curve Diffie-Hellman 키 교환(ECDH) 과정으로 비밀 값 Z 를 공유하고 이후 키 확인 과정(MacTagA, MacTagB) 수행
② SSE 과정에서 키 공유와 확인 과정이 성공적으로 수행되면 SCH 과정 진행
③ NFC 기기는 데이터의 기밀성과 무결성을 제공을 위해 암호 키와 무결성 키를 비밀 값 Z 와 랜덤 값 등으로부터 유도하여 공유
④ 생성된 암호키와 무결성 키를 이용하여 NFC 기기간의 데이터를 AES-CTR 모드로 암복호화 및 AES-CBC 모드로 무결성 확인

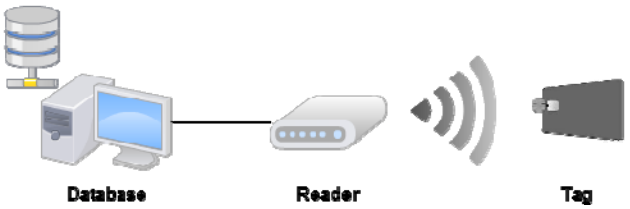
추가적으로 ECMA 에서는 NFC 기기에서 보안 서비스를 제공하기 위한 암호학적 함수들을 <표 1>과 같이 정의 하였다[6].

<표 1> ECMA-386 암호학적 함수

과정	암호학적 함수
보안 서비스	SSE(Shared Secret Service) SCH(Secure Channel Service)
키 공유	ECDH P-192
키 유도 함수	AES-XCBC-PRF-128
키 확인	AES-XCBC-MAC-96
기밀성	AES 128-CTR IV init :AES-XCBC-PRF-128
무결성	AES-XCBC-MAC-96
재생 공격 방지	SN(Sequence Number)

3. 기존 RFID 환자 인증 시스템

일반적으로 RFID 시스템은 그림 4 와 같이 백-엔드 데이터베이스 서버(DB), RFID, 리더(Reader), RFID 태그(Tag)들의 3 종류의 컴포넌트들로 구성되어 있다.



(그림 4) 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 채널이며 리더와 태그 간의 채널은 안전하지 않은 채널로 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 서버로 전달한다. DB 서버는 자신의 DB 테이블 정보와 리더로부터 수신한 정보를 이용하여 태그를 인증한 후, 해당 태그에 관한 제품 정보 등을 리더에게 알려준다. RFID 시스템에서 보안 요구 사항은 크게 익명성, 위치 프라이버시, 재전송 공격, 스푸핑 공격, 위치 트래킹 공격에 대한 안전성 보장이 있다[1,2].

대부분의 RFID 환자 인증 시스템에서는 데이터베이스 서버 내에 저장된 태그들의 비밀 정보를 안전하게 보호하기 위한 DB 정보 암호화 기법을 사용하고 있다.

암호화 기법으로는 해쉬 함수와 메시지 인증 코드를 이용하거나 암호화 알고리즘인 AES, DES 를 사용하여 키 추출 공격에 방어하여 보안성을 증명하고 있다[1,2]. 하지만 이러한 RFID 시스템의 보안성 강화에도 해결되지 않는 문제는 RFID 태그 자체의 낮은 연산 능력과 낮은 저장공간으로 인한 단방향 암· 복호화 알고리즘 적용으로 인한 키 추출 공격에 대한 방어가 어려울 뿐만 아니라 도청, 데이터의 위• 변조 공격이 가능해 진다. 이러한 RFID 환자 인증 시스템의 취약점을 보완하기 위한 방법으로 본 논문은 NFC 기반 환자 인증 시스템을 제안하고자 한다.

4. NFC 기반 환자 인증 시스템 설계

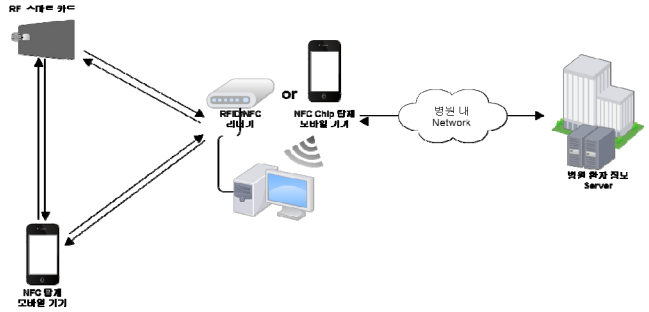
RFID 의 취약한 보안성을 강화한 NFC 기술을 적용으로 환자 정보 보호는 물론이거니와 병원 관계자의 업무 효율성을 제공할 수 있는 시스템을 본 논문에서 제안하고자 한다

우선 RFID 의 적은 메모리로 인한 정보 저장의 제약성과 낮은 연산 능력으로 인한 보안 알고리즘을

적용 불가에 대한 해결은 NFC 가 보완하고 있다.

NFC 기술의 특징인 쌍방향성 통신과 NFC 스마트 기기의 메모리 공간을 이용한 데이터 저장의 제약을 해결해 줄 수 있을 뿐 만 아니라, 데이터 무결성 및 기밀성을 위한 암호화 알고리즘을 적용을 할 수 있는 큰 장점을 가지고 있다.

본 논문에서 제안하는 NFC 기반 스마트 기기 환자 인증 시스템의 전제 구성도는 다음 그림 5 와 같다.



(그림 5) NFC 기반 환자 인증 시스템 전체 구성도

NFC 는 RFID 기술의 파생된 기술로 호환성을 지니고 있기 때문에 기존의 환자 RF 스마트 카드의 식별 정보를 NFC 모바일 기기를 통해 읽어와서 사용이 가능하게 된다. 반대로 NFC 는 기록 모드가 가능하기 때문에 RF 스마트 카드 정보를 기록하는 역할도 병행할 수 있다.

인증 절차의 시나리오를 설명하자면 우선 병원 환자 정보 DB 에 환자의 RF 스마트카드 또는 NFC 모바일 기기 간의 고유 식별 정보를 사전에 생성시키는데, 이를 대칭키 암호화 알고리즘을 통해 키를 발급하여 인증에 사용되도록 한다.

이렇게 부여받은 환자 식별 번호를 가진 모바일 기기(=클라이언트)를 기존의 RFID/NFC 리더기 또는 의사의 NFC 모바일 기기를 통해 태그를 하면, 인증에 필요한 키 정보를 읽어 들여 환자 정보 서버에 인증 절차를 거치게 된다. 환자 정보 DB 에서 인증 확인 후 Success 또는 Failed 메시지를 클라이언트에 보낸다.

제안하는 시스템에서는 기존의 RFID 시스템과는 달리 DB 뿐만 아니라 NFC 태그에도 암· 복호화 알고리즘과 해쉬 알고리즘 적용함으로써 키 추출에 대한 방어를 강화하여 데이터의 무결성 및 기밀성을 보장할 수 있다는 점을 강조하고자 한다.

따라서 제안하는 NFC 기반 모바일 기기 환자 인증 시스템을 통해 정확한 환자 인증과 환자의 개인정보 누출과 같은 보안성 강화, 그리고 의료 관계자의 업무 효율성을 제공해 줄 수 있다[3].

5. 결론 및 연구 방향

최근 의료계에서 의료 사고 방지를 위해 RFID 와 같은 근접 무선 통신 기술을 적용함으로써 의료 기술 선진화를 도모하고 있지만, 개인 정보와 같이 민감한 정보가 누출 되는 기술적 취약점 발견으로 인해 보안성 강화가 필요하게 되었는데, 이를 보완 및 대안을 위해 본 논문은 NFC 기반 환자 인증 시스템을 제안하였다. NFC 는 새로운 기술이 아닌 RFIC 기술에서 파생되어 나온 기술로써 10cm 범위 내 통신을 지원하는 초근접 무선 통신 기술이다. 타 통신기술 보다 짧은 거리로 인해 원거리 해킹 공격에 대한 보안성은 타 기술보다 뛰어나다고 할 수 있다. 또한 NFC 기술의 특징인 양방향 통신이 가능하며, Reader/Writer 모드를 통한 태그 리더기 및 기록이 가능하여 활용도가 매우 높다[5].

그리고 NFC Chip 을 탑재한 모바일 기기를 통해 많은 정보를 저장 할 수 있으며, 암호화 알고리즘을 적용이 가능해 개인 정보 보호에 필요한 보안성을 강화할 수 있는 요건을 갖추고 있다.

이러한 NFC 장점을 토대로 기존 RF 스마트 카드를 이용한 환자 인증 시스템에 NFC 기술을 접목하여 보안성과 효율성을 높일 수 있게 된다.

향후 연구 방향은 NFC 기술의 3 가지 모드를 병원 정보 시스템과의 연동을 통해 더 많은 의료 서비스 모델 및 개발에 대한 연구가 필요 할 것으로 보인다.

참고문헌

[1] 윤은준, 유기영. “의료정보보호를 위한 RFID 를 이용한 환자 인증 시스템”. 한국통신학회. 2010. 6.

[2] 박종혁, 강수영. “U-Healthcare 환경에서의 RFID 정보보호이슈에 관한 고찰”. 보안공학연구논문지. 2008.10

[3] 이민구, 김동완 외 1 인. “NFC 를 활용한 능동형 인증 방법”. 한국통신학회. 2012.2

[4] 이재식, 김형주 외 3 인. “NFC 환경에서 개인정보 보호를 위한 취약점 분석 및 대책 수립 방법론”. 과학기술학회 2012. 4

[5] 김연우, 문일영. “NFC 의 기술 동향 분석 및 활용 사례”. 한국해양정보통신학회. 2011.

[6] 박재영, 김용강 외 2 인. “NFC 모바일 폰을 활용한 도서관 시스템”. 한국정보과학회. 2011.11.

[7] 임선희, 전재우 외 2 인. “NFC 보안 기술 분석 및 UICC 적용 효과 연구”. 한국통신학회. 2011.1

[8] 김선배, 김형국 외 1 인. “NFC 에서의 보안 취약점 분석”. 한국인터넷정보학회. 2011.