

# NFC를 활용한 출입 통제 시스템

김덕경, 양환석, 이병천

중부대학교 정보보호학과

## Access Control System using NFC

DeokKyung Kim, HwanSeok Yang, Byoungcheon Lee

Dept. of Information Security, Joongbu University

### 요약

최근 스마트폰의 NFC(Near Field Communication)기능이 광고, 티켓팅, 의료서비스, 안내/제품 정보, 결제 및 계좌이체, 개인인증 등 많은 분야에서 활용되고 있다. 그 중 개인인증분야의 출입문 개폐(도어락)를 보면 현재 대부분의 회사에서의 출입통제에 RFID(Radio Frequency Identification) 카드(사원증)와 리더기를 이용하고 있다. 그러나 이러한 RFID 카드를 사용하는 출입통제는 분실의 위험이 다소 높으며 리더기에 사용자 정보를 저장함으로써 악의적인 해킹에 노출되어 있고, 또 리더기 설치에 많은 비용이 발생하기 때문에 NFC를 활용한 출입통제 시스템에서는 기존 출입 단말기 대신 NFC 태그를, 기존 사원증 형태의 RFID 카드 대신 스마트폰의 NFC 기능을 이용하여 출입통제를 할 수 있도록 설계 및 구현하였다.

NFC를 활용한 출입통제 시스템을 구현하기 위해서 관리자, 사용자 스마트폰 어플리케이션을 구현하고 Apache, PHP, MySQL을 이용해 서버와 데이터베이스를 구축하였으며 자바를 이용하여 관리자 프로그램을 구현하였다.

### I. 서론

스마트폰, 태블릿 PC 등 2010년부터 폭발적으로 보급된 스마트 디바이스의 영향으로 모바일 결제 분야에서 가장 중요한 이슈로 떠오른 기술은 NFC 기술이다. NFC 기술은 2004년부터 표준이 개발되었지만 이를 적용할 디바이스 및 서비스의 부재로 활용이 되고 있지 않다가 2011년 구글이 구글웰렛 서비스를 시작하면서 본격적으로 NFC 기반 서비스가 적용되기 시작하였다. 이러한 스마트 디바이스의 확산과 무선 네트워크의 발전은 우리의 일상생활을 윤택하고 편리하게 변화시켜 나가고 있으며 앞으로는 다양한 분야로 지속적으로 확산되어 갈 것으로 예상된다[1]. 또한, NFC 기반 통신 기능을 채용한 스마트기기 및 OS 등이 확산됨에 따라 기존 RFID를 이용하던 다양한 응용 분야에 대하여 NFC로의 대체가 진행되고 있다. 개인 인증 분야에서도 기존 RFID 카드 대신 NFC로 대체되고 있는데 본 논문은 스마트폰의 기능 중 하나

인 NFC를 이용하여 사원증 소지의 불편함과 리더기 설치 시의 비용, 기존 리더기에 사용자 정보를 저장함으로써 악의적인 해킹에 노출되어 있는 문제를 해소하고자 출입통제 시스템을 설계 및 구현하였다.

본 논문은 다음과 같이 구성된다. 2장에서는 RFID와 NFC 기술에 대해 소개한다. 3장에서는 NFC를 활용한 출입 통제 시스템의 설계 및 구현을 소개한다. 4장에서는 결론 및 향후 연구 방향을 제시한다.

### II. 관련연구

#### 2.1 RFID

사물에 전자태그를 부착하여 사물의 정보를 인지하고 이를 전송하는 RFID시스템은 유비쿼터스 컴퓨팅을 구현할 중요한 기술요소로 각광받고 있다. RFID시스템은 크게 마이크로칩을 내장한 Tag와 태그에 저장된 데이터를 무선주파수를 이용하여 인식(Read/Writer)하는 리더(Reader), 그리고 인식한 데이터를 송·수신하는

안테나로 구성되는 일종의 무선통신시스템이다. RFID 태그는 물품, 의류, 자동차 등에 부착되어 이동하며 지상이나 건물에 고정되어 있는 안테나와 무선 통신을 수행한다. 이때 리더는 안테나와 RFID 태그의 통신을 제어하거나 컨트롤러(Controllor)와 RFID사이의 프로토콜을 교환하는 기능을 담당한다. 이에 RFID는 기존의 바코드나 자기 인식 장치의 단점을 보완하고 사용의 편리성을 향상시킴으로서 물류 및 유통, 농업, 의료, 전자도서관, 금융, 보안 교통, 홈 네트워크 등 산업 전반의 다양한 분야에 적용되는 차세대 핵심기술의 하나로 주목받고 있다[2].

## 2.2 NFC

무선근접통신을 의미하는 NFC는 전자태그(RFID)의 일종으로 13.56MHz 주파수 대역을 사용하여 비접촉식으로 10cm 이내의 단거리에서 기기간 데이터를 전송하는 기술이다. NFC 기술은 기존의 비접촉식 스마트카드 기술(ISO/IEC 14443 Proximity-card 표준)을 기반으로 개발되었으나 단순 스마트카드 기능뿐 아니라 양방향 통신을 통해 전자태그의 정보를 읽어오거나 반대로 정보를 입력할 수 있는 Read/Write 기능과 단말 간 통신을 위한 P2P 기능까지 제공한다. 신용카드, 신분증 등을 대체할 수도 있으며, 노트북의 사용자 인증, 모바일 티켓, 쿠폰 등 다양한 분야에서 활용될 수 있는 성장 잠재력이 큰 기술이다. [3,4,5]

NFC 포럼[6]에서는 NFC의 주요 응용대상 분야를 ①기기간 통신(P2P), ②리드/태그(R/W), ③카드 에뮬레이션(SC)의 세 가지로 분류하고 각각의 동작에 필요한 기술요소들을 표준화하고 있다.

- P2P모드:ISO/IEC 14443 A + FeliCa
- R/W모드:ISO/IEC 14443 A/B + FeliCa
- SC모드:ISO/IEC 14443 A + FeliCa

## III. 접근통제 시스템 설계 및 구현

본 논문에서는 NFC 기능을 장착한 스마트폰의 R/W 기능과 NFC Tag를 이용하였고 구현하기 위하여 안드로이드, Apache, PHP, MySQL, 자바를 이용했다.

스마트폰 어플리케이션은 관리자용과 사용자

용을 각각 구현하였다. 관리자 어플리케이션은 NFC Tag에 사무실 정보를 입력하는데 사용되고 사용자 어플리케이션은 NFC Tag에서 받은 사무실 정보와 함께 사용자 정보, 현재 시간을 출입통제 서버로 전송한다.

출입통제 서버는 사용자 어플리케이션으로부터 받은 정보를 MySQL과의 질의를 통해 인증 여부를 확인하여 출입승인 여부를 결정한다. NFC를 활용한 출입통제 시스템은 출입문 개폐 장치와 직접 연동하지는 않았고 출입승인정보를 서버에 XML 파일로 저장하고 사용자 스마트폰에 XML파일을 읽어와 출입승인 여부를 표시하는 형태로 구현했다.

자바 프로그램은 관리자용 프로그램으로써 관리자가 사용자 정보관리 및 출입조회를 쉽게 할 수 있도록 구현하였다.

그림1은 출입통제 시스템의 전체 설계를 나타낸 것이다.



그림1. 출입통제시스템의 구성도

### 3.1 관리자 및 사용자 어플리케이션



그림2. 어플리케이션

사무실 정보를 NFC Tag에 저장하는 용도이다. makeReadOnly() 함수를 이용하여 한번

NFC Tag에 저장된 정보는 수정 및 삭제가 불가능하다(왼쪽).

관리자 어플리케이션의 동작은 다음과 같은 형태로 수행된다.

① 스마트폰의 NFC 기능을 활성화 한 후 '사무실 번호 입력'란에 알맞은 정보를 입력한다.

② save 버튼을 누르면 "Tag에 가까이 하세요" 라는 창이 뜬다.

③ 스마트폰을 NFC Tag에 태깅한다.

스마트폰을 NFC Tag에 태깅 시 출입승인여부 정보를 확인 할 수 있다. 사용자 인증결과에 따라 출입승인여부 정보가 표시된다(오른쪽).

사용자 어플리케이션의 동작은 다음과 같은 형태로 수행된다.

① NFC Tag에 스마트폰을 태깅 시 NFC Tag에 있는 사무실 정보를 스마트폰이 읽어온다.

② 읽어온 사무실 정보와 사용자 정보(스마트폰 번호, 현재 시간)를 출입통제 서버에 url.openstream을 이용하여 전송한다.

③ 출입통제 서버에서는 DB와의 질의 후 출입승인여부를 XML파일 형태로 저장하는데 사용자 어플리케이션은 이것을 읽어와 승인여부를 화면에 표시한다.

현재까지는 개폐기능을 연동할 수 있는 장치가 없어서 개폐기능을 구현하지 않았으며 대신 사용자 스마트폰 화면에 승인 여부를 표시하도록 했다. 출입문의 개폐장치와 연동하면 실제 출입관리 시스템으로 이용 가능하다.

### 3.2 출입통제 서버

출입통제 서버는 APMSetup을 이용해 PHP로 구축하였고 스마트폰에서 넘어온 사용자 정보를 DB와 질의 후 인증한다.

```
while($obj = mysql_fetch_object($result))
{
    $check_num=$obj->phone;
    $check_level=$obj->level;
    $check_name=$obj->name;
    $check_idx=$obj->idx;
}
if($check_num != NULL) {
    while($obj = mysql_fetch_object($result1))
    {$office_level=$obj->level;}
    if($office_level>=$check_level)
    {
        $xmlcode .="<phonenum>$check_num</phonenum>\n";
        $xmlcode .="</user>\n";
        $filename = $dir."/insert.xml";
    }
}
```

### 3.3 MySQL DB 구성

DB는 사용자 정보 테이블, 사용자 출입 관리 테이블, 사무실 정보 테이블로 구성되어 있다.

| 구분 | 컬럼명  | 컬럼 ID | DATA TYPE | 길이 | 비고          |
|----|------|-------|-----------|----|-------------|
| 1  | 사원번호 | Idx   | Varchar   | 20 | 1111111     |
| 2  | 이름   | Name  | Varchar   | 15 | 김덕경         |
| 3  | 번호   | Phone | Varchar   | 20 | 01012345678 |
| 4  | 보안등급 | level | Varchar   | 15 | 1           |

그림3. 사용자 정보 테이블

| 구분 | 컬럼명  | 컬럼 ID  | DATA TYPE | 길이 | 비고                |
|----|------|--------|-----------|----|-------------------|
| 1  | 사원번호 | Idx    | Varchar   | 20 | 1111111           |
| 2  | 이름   | Name   | Varchar   | 15 | 김덕경               |
| 3  | 사무실  | Office | Varchar   | 20 | 415               |
| 4  | 출입시간 | Time   | Varchar   | 15 | 2014/04/17 /17:20 |

그림4. 사용자 출입 관리 테이블

| 구분 | 컬럼명  | 컬럼 ID  | DATA TYPE | 길이 | 비고  |
|----|------|--------|-----------|----|-----|
| 1  | 사무실  | Office | Varchar   | 20 | 415 |
| 2  | 보안등급 | Level  | Varchar   | 15 | 1   |

그림5. 사무실 정보 테이블

### 3.4 관리자 프로그램

자바로 만들어진 관리자 프로그램은 SWING을 이용한 GUI 프로그램으로 제작하였다.

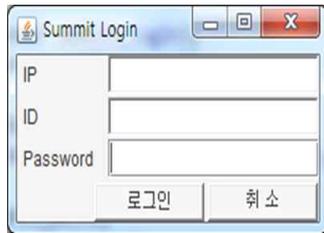


그림6. 관리자 프로그램 로그인

관리자는 먼저 서버 아이피, 관리자 아이디, 패스워드를 입력해 로그인을 한다(그림6).



그림7. 사용자 정보 관리

사용자를 등록할 수 있고, 수정, 삭제, 조회할 수 있다(그림7).



그림8. 사용자 출입 조회

사용자 출입조회 창으로써 사원번호, 이름, 사무실, 출입일시를 이용하여 조회 할 수 있다. (그림8).

관리자는 새로운 사용자를 등록할 수 있고, 사용자 정보를 조회, 수정, 삭제할 수 있다. 출입 조회 버튼을 누르면 사용자가 태깅 시 남겨지는 출입 정보를 확인 할 수 있으며 검색기능

을 이용하여 편리한 관리가 가능하다. 그림8은 사용자의 정보를 등록, 수정, 삭제, 조회할 수 있는 화면을 나타낸다.

#### IV. 결론

본 논문에서는 관리자가 관리자 어플리케이션을 통해 쉽게 NFC Tag를 관리하고 자바로 만든 관리자 프로그램을 이용하여 사용자의 정보관리, 출입조회를 손쉽게 할 수 있고 사용자는 사용자 어플리케이션을 이용하여 간편한 인증을 할 수 있다. NFC를 활용한 출입통제 시스템을 구현하기 위해 학교내 와이파이를 이용하여 서버와 안드로이드 간의 통신을 테스트해 정상적으로 구현하였다.

스마트폰은 사용자가 항상 휴대하고 다니는 물품이므로 분실에 대한 우려가 상대적으로 낮아서 인증용 도구로 유용하다. 현재까지는 스마트폰에 내장된 사용자의 휴대폰번호만으로 인증이 가능하도록 구현하였지만 향후 스마트폰에 저장된 공인인증서와 이를 이용한 전자서명을 이용하는 인증 방식 또는 2차 비밀번호 인증 방식 등의 방식으로 사용자와 서버간의 인증에 보안 강화를 고려해야 한다.

#### [참고문헌]

- [1] 백종현, 염홍열, "NFC 기반 모바일 서비스 보안 위협 및 대책" 정보보호학회지 제23권 제2호, 55-65, 2013.
- [2] 강유성, 최두호, 김호원, "모바일 RFID 보안 기술 표준화 동향 및 표준화 추진 전략", 전자통신동향분석 제23권 제2호, 142-152, 2008.
- [3] 김형준, 권태경, "NFC 기술 동향과 보안 이슈", 한국통신학회지 (정보와 통신) 제29권 제8호 57-64, 2012.
- [4] 나성욱, 이윤희, 지정순, "스마트폰과 모바일 오피스의 보안 이슈 및 대응 전략", CIO Report 26권 28p ISSN 2092-6944.
- [5] ISO/IEC 21481:2005 Near Field Communication Interface and Protocol-2 (NFCIP-2), ISO/IEC,NFC
- [6] 김경식, 신준호, "NFC 기술 및 인증동향", TTA journal / no.133, 2011년, pp.132-136