보안 기능이 강화된 NFC 기반 사용자 맞춤형 태깅 서비스 구현

안혜준, 원예은, 정세영, 김명주
서울여자대학교 정보보호학과
e-mail:dkshj0815@swu.ac.kr

Implementation of Security-enhanced NFC-based Tagging Service supporting Customizing Feature

Hye-Jun Ahn, Ye-Eun Won, Se-Young Jung, Myuhng-Joo Kim
Dept. of Information Security, Seoul Women's University

요 약

본 연구에서는 다양한 서비스에 안전하면서도 쉽게 사용할 수 있는 NFC 태깅 서비스 앱을 개발하였다. 이 앱을 활용하면 NFC 태깅만으로도 복합 동작을 한 번에 수행할 수 있고 일상의 실물 하드웨어에 대한 직접 제어도 가능하여 NFC를 사용자가 지정한 다양한 분야에 걸쳐 쉽게 사용할 수 있다. 아울러 간편하면서도 안전한 사용자 인증과 NFC 활용을 위하여 암호화 기반의 보안 기능도 제공한다.

1. 제작배경

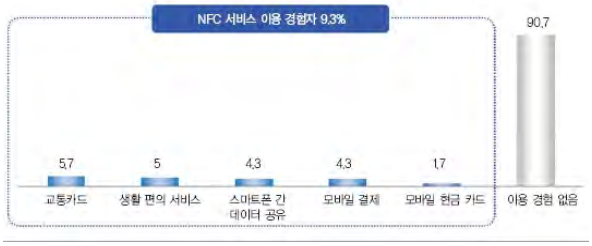
바쁜 일상을 살아가는 사람들을 위해 편리하고 간단한 동작들을 스마트폰을 사용하여 제공하는 서비스들이 증가하고 있다. 특히 간편 결제와 같이 단순 처리를 제공하는 서비스들의 경우 대부분은 스마트폰의 NFC 서비스를 사용하여 제공한다. NFC(Near Field Communication)는 10cm 이내의 근거리에서 데이터 전송을 지원하는 비접촉식 무선통신의 한 기술이다[1]. 다음 (그림 1)에서 보는 것과 같이 NFC를 탑재한 스마트폰의 출하량 전망이 증가하는 것을 볼 수 있다[2].

(그림 1) NFC가 탑재된 스마트폰 출하 현황

이러한 NFC가 탑재된 스마트폰의 급속한 확산으로 인해 NFC에 기반을 둔 앱들이 다양하게 출현하고 있다. 예를 들어, 출입통제, 헬스케어, 정보수집 등에 걸쳐 NFC의 활용 분야는 점차 다양해지고 있다[3].

본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 SW중심대학지원사업의 연구결과로 수행되었음(2016-0-00022)

반면에 이용자들이 NFC를 사용하는 분야는 상대적으로 제한적임을 다음 (그림 2)는 보여주고 있다.



(그림 2) 사용자 측면의 NFC 서비스 이용 현황

사용자들은 NFC를 주로 결제수단으로 사용함을 알 수 있는데 이는 NFC 관련 앱의 사용법이 갈수록 복잡해지며 사용에 보안 침해 염려가 존재하기 때문이다[4]. 본 연구에서는 일상의 복잡하면서도 다양한 서비스에 NFC를 간단하면서도 안전하게 사용할 수 있는 앱을 구현하였다.

2. 유사 앱들의 비교

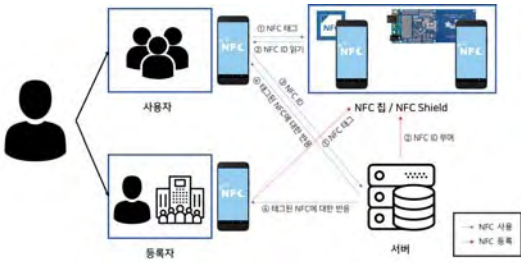
<표 1> 기존에 나와 있는 NFC 앱 비교

앱	읽기, 쓰기	간단 기능 (URL 연결, 앱 연결)	와이파이, 블루투스	전화, 문자	영상, 녹음 공유
	O	X	X	X	X
	O	O	O	O	X
	O	O	O	X	O
	O	O	O	X	O
	O	O	O	O	X

<표 1>은 앱시장에서 나온 기존 앱들 비교한 것이다[5, 6, 7, 8, 9, 10, 11, 12, 13]. 기존 앱들은 주로 NFC의 일반적인 기능인 읽기와 쓰기를 다루고 있으며, 기능이 확장될 경우 URL 및 다른 앱 연결을 지원함을 알 수 있다.

이러한 기존의 앱들은 대부분 서비스를 고정 제공하는 반면, 본 연구에서는 사용자가 주는 정보와 받는 정보를 선택함으로써 맞춤형 정보를 송수신할 수 있도록 한다. 뿐만 아니라 일상에 존재하는 다양한 하드웨어를 단순한 NFC 태킹 동작만으로 직접 제어할 수 있는 기능도 제공한다. 아울러 이러한 서비스가 안전하게 이루어지도록 보안 기능도 제공하여 기존 앱과 차별되도록 설계한다.

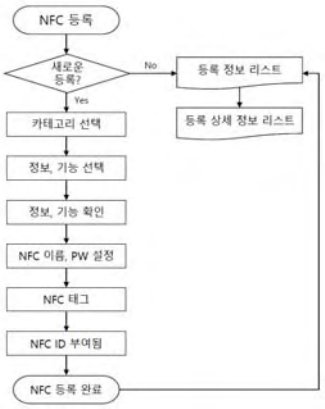
3. 시스템 구성도



(그림 3) 시스템 구성도

본 연구에서 개발한 앱의 사용자는 (그림 3)이 보여주는 것과 같이 NFC 등록자 역할과 NFC 사용자 역할을 모두 할 수 있다. NFC 등록자는 사용에 따른 다양하고 복잡한 기능을 선택적으로 등록할 수 있으며, 이러한 기능을 저장하고 서버로부터 NFC ID를 부여받는다. NFC 사용자는 앞서 등록되어있는 NFC를 단순하게 태깅함으로써 지정된 NFC ID 별로 선택적인 응답 서비스를 받게 된다.

4. NFC 등록과정



(그림 4) NFC 등록 순서도

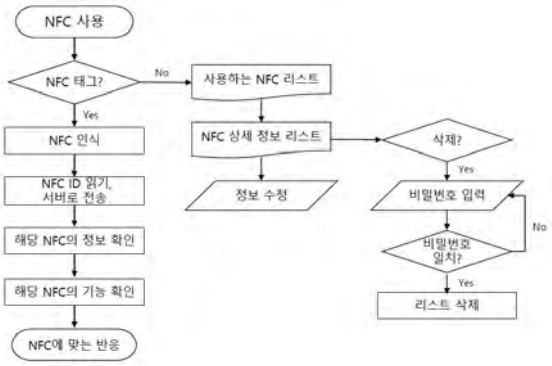
NFC를 사용하기 이전에 특정 NFC를 어떤 기능으로 사용할 것인지 사전 등록이 필요하다. (그림 4)는 등록자가 앱을 이용하여 NFC를 등록하는 과정이다[14, 15].

NFC 등록을 할 때 어떤 기능인지에 따라 과정이 다르기 때문에 카테고리를 우선적으로 선택한다. 카테고리는 NFC가 적용될 수 있는 분야들을 구분한 것으로, 크게 간단 기능, 앱 연결, 신원 확인, 하드웨어 연결 네 가지로 구성된다. 간단 기능은 와이파이 연결, 무음/진동 변경, 명함 교환, 파일 다운로드처럼 NFC를 이용하여 할 수 있는 간단한 기능을 말한다. 앱 연결은 태그를 했을 때 날씨 앱, 멤버십 앱 등 다른 앱을 띄우는 카테고리이다. 신원 확인은 근태 관리, 출결관리 등 신원을 확인해야 하는 NFC를 만드는 카테고리이고, 하드웨어 제어는 출입문, 택배 보관함, 전등과 같은 하드웨어를 연결할 경우에 사용한다.

등록자는 NFC의 기능을 수행하기 위해 필요한 정보들을 선택한다. 이때, 해당 기능을 사용하기 위해 필수적 정보인지 선택적 정보인지 구분한다. 더불어, 정보들이 사용자가 태그를 했을 때 등록자가 사용자에게 보내는 정보인지, 등록자가 사용자로부터 받는 정보인지 구분한다. 이후, NFC 태그 시 수행할 기능을 선택한다. 예를 들어, 출결 NFC를 등록한다고 하면, 필수 정보는 이름과 학번이고, 선택 정보는 전화번호 등이 될 것이다. 기능도 태그를 했을 때 무조건적으로 수행되는 기능과 사용자가 선택할 수 있는 기능이 있다.

NFC를 사용하는데 필요한 정보와 기능을 모두 설정하면, 등록할 NFC를 스마트폰에 태그한다. 태그가 제대로 인식되면 서버에서 NFC ID를 부여함과 동시에 DB에 저장된 후 NFC 칩에 NFC ID가 입력된다. 이는 사용자가 NFC를 태그 했을 때 어떤 NFC인지 구분할 수 있는 지표가 된다. NFC ID가 성공적으로 입력되면 NFC 등록이 완료된다. 이후, 등록한 NFC를 리스트로 볼 수 있고 상세 내용을 확인, 수정, 삭제할 수 있다. 등록자가 NFC를 삭제하면 해당 NFC는 사용자 목록에서도 삭제된다.

5. NFC 사용절차

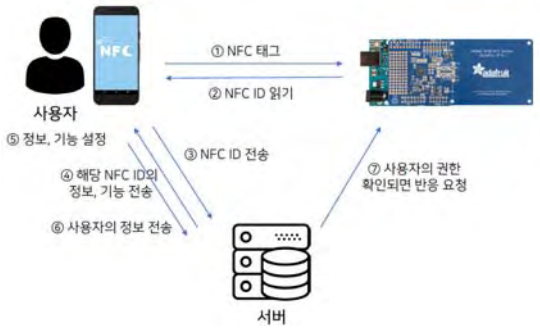


(그림 5) NFC 사용 순서도

(그림 5)는 사용자가 앱을 이용할 때 NFC를 사용하는 과정을 보여준다. 스마트폰의 NFC 통신 기술에서 제공하

는 읽기/쓰기 모드는 기본적으로 제공된다[16]. 사용자가 앱을 실행하여 태그를 하면 NFC의 읽기 모드를 사용하여 NFC ID를 읽어온다. 읽힌 NFC ID는 변수로 받아 서버와 연결한다. 서버로 전송된 NFC ID가 서버에 존재한다면, 서버 DB에서 NFC ID와 맞는 정보와 기능을 앱으로 전송한다. 전송된 정보를 앱에서 받아 사용자에게 화면을 통해 띄운다. 이 경우 화면을 통하여 서버 DB에서 받아온 NFC 등록자가 설정한 정보와 기능을 보여준다. 등록자가 선택 정보를 사용하였다면, 사용자는 화면에 보이는 ON, OFF 버튼을 통해 선택한다. 선택된 정보를 통해 등록자에게 자신의 정보를 보낸다. 기능도 정보와 같이 등록자가 선택할 수 있도록 설정하였다면, 자신이 원하는 기능을 선택할 수 있다. 기본적으로는 등록자가 등록 시 설정한 기능이 수행되는데, 사용자가 자신이 원하는 기능을 선택하여 하드웨어를 직접 제어할 수 있다. 이처럼 본 앱은 사용자가 원하는 기능들을 선택할 수 있는 맞춤형으로써, 사용했던 NFC들을 확인할 수 있으며 변경하고 싶다면 수정을 통해 변경할 수 있다. 더 이상 쓰지 않는 NFC는 비밀번호를 통해 자신의 앱에서 지울 수 있다.

6. 하드웨어 직접 제어 기능



(그림 6) NFC를 이용한 하드웨어 제어 과정

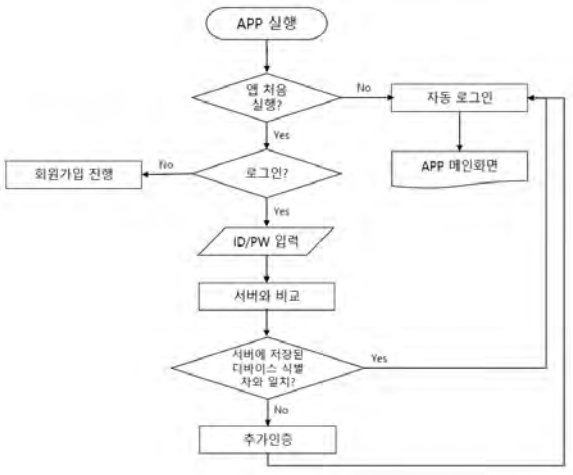
NFC 태그로 하드웨어를 직접적으로 제어할 수 있다[17, 18, 19]. Arduino UNO R3와 Adafruit NFC Shield를 이용하여 구현하였다. 하드웨어를 제어하는 과정은 다음과 같다. ① 사용자는 NFC를 사용하기 위해 NFC Shield에 NFC가 켜진 스마트폰을 태그한다. ② 태그가 제대로 인식되면 NFC Shield 안에 있는 NFC ID가 읽힌다. 이때 NFC ID는 등록자가 등록할 때 서버가 부여한 고유의 ID이다. ③ 하드웨어로부터 읽은 NFC ID를 서버에 보낸다. ④ 서버는 받은 NFC ID가 DB에 있는지 확인한다. NFC ID가 있다면, 해당 NFC가 요구하는 정보와 기능을 사용자의 앱 화면에 띄운다. NFC ID가 없다면, 태그한 하드웨어는 아직 등록이 안 되어있는 것이므로 제어가 불가능하다. ⑤ 사용자는 앱에서 하드웨어 제어를 위해 필요한 정보와 기능을 확인한다. 이때, 사용자는 선택 정보를 전송할 것인지 선택할 수 있다. ⑥ 사용자가 앱에서 설정 완료 버튼을 클릭하면 사용자가 설정한 정보와 기능이 서버에 보내진다. ⑦ 서버는 사용자의 정보를 받고 권한을 확인한다. 권한이 있는 사용자라면, 서버는 하드웨어에 사용자가 설정한 기능을 수행하도록 요청한다. 이 과정을 통해 사용자는 하드웨어를 제어할 수 있다.

이와 같은 방식으로 NFC 태그를 인식할 수 있는 하드웨어를 이용하면 형광등 켜고 끄기, 택배 보관함 여닫기, 현관문을 잠그고 해제하기 등이 가능하다. 이처럼 항상 지니고 다니는 스마트폰으로 하드웨어를 제어한다면 더욱 편리한 생활이 가능할 것이다.

7. 안전한 이용을 위한 보안 조치

프로젝트에서 중요한 기능인 본인인증에 대한 신뢰성을 확보하기 위한 방법과 서버와 클라이언트 통신 시 일어날 수 있는 문제를 예방하는 방법으로 나눠 살펴볼 것이다.

7.1 신뢰성 보장

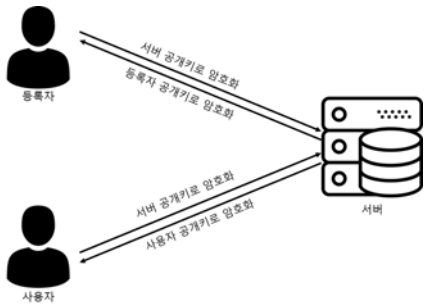


(그림 7) 신뢰성 보장을 위한 순서도

앱이 처음 실행(처음 설치, 재설치)되면 로그인 화면으로 넘어가고 재실행이라면 자동 로그인을 통해 앱 메인 화면으로 넘어간다. 로그인 화면에서 회원가입을 누르면 회원가입 창으로 넘어간다. 만약 회원가입 하지 않고 ID와 PW를 입력하면 서버와 비교해 ID가 있는지 판별한다. ID가 서버에 저장되어 있다면 그 ID에 해당하는 디바이스 식별자가 현재 사용하는 디바이스 식별자와 일치하는지 확인하는 과정을 거친다. 일치한다면 자동 로그인을, 아니라면 이메일이나 SMS 등을 통한 추가 인증을 실시해 본인임을 확인한 후에 자동 로그인이 진행된다[20].

1기기 1계정을 기본으로 하며, 기기 변경, 앱 재설치, 제3자의 무단 사용 등을 막기 위해 (그림 7)과 같은 순서도를 작성하였다.

7.2 통신 보안



(그림 8) 통신 시 암호화

사용자와 서버간의 통신에는 개인정보가 오고 가기 때문에, 공개키 암호화를 사용하여 패킷이 오고 갈 때 패킷 스니핑 등으로 인한 개인정보 누출을 방지한다. 사용자가 등록자에게 정보를 보낼 때는 서버의 공개키로 암호화한다. 그 후 서버에서 서버의 개인키로 복호화한 후, 등록자의 공개키로 암호화해 공격자에게 전송한다. 등록자는 서버로부터 받은 암호문을 등록자의 개인키로 복호화해 확인한다. 마찬가지로 공격자가 사용자에게 응답을 보낼 때 서버 공개키로 암호화한다. 그 후 서버에서 서버의 개인키로 복호화한 후, 사용자의 공개키로 암호화해 사용자에게 전송한다. 받은 암호화된 응답을 사용자의 개인키로 복호화해 내용을 확인한다.

8. 기대효과

이 연구 결과물을 통하여 다음과 같은 효과를 기대할 수 있다.

첫째, NFC 사용 가능 영역을 다양하게 확장할 수 있다. 지금까지 보급된 NFC 앱들처럼 간단한 기능을 수행하는 것뿐만 아니라 NFC 태그별로의 응답을 다르게 해 양방향 통신이 가능하도록 하고, 아두이노를 통한 하드웨어 제어가 가능하다[21].

둘째, 반복되는 복잡한 작업들이 간소화될 것이다. 아침마다 수행해야 했던 여러 가지의 일들을 태그 한 번으로 모두 수행하게 할 수 있다.

셋째, 사용자 각자의 상황에 맞추어 기능 설정이 가능하다. 같은 NFC를 쓰더라도 추가정보 전송에 대한 선택권과 그에 따른 반응을 선택할 수 있다. 이로 인해 태그로 인한 과도한 정보 유출을 막을 수 있다[22].

넷째, 본인인증이 안전하면서도 간편해진다. 다양한 페이지를 접속할 때마다, 로그인해야 하는 번거로움을 NFC 태깅만으로 본인인지 구분해낼 수 있는 정보들을 통해 쉽게 본인인증이 가능해진다.

이상의 효과를 고려할 때 본 연구에서 개발한 NFC 앱을 통하여 일상의 더욱 다양한 분야에서 사용자들의 다양한 선택권을 지원하면서 안전하고 편리하게 NFC의 기능을 활용할 수 있을 것으로 기대된다.

참고문헌

[1] 한영선, “NFC 표준 기술 분석 및 전망”, 한국멀티미디어학회지, 16(3), pp. 17-23, 2012.9

[2] 김대건, “O2O 동향과 시사점”, 정보통신방송정책, 26(22), pp. 1-20, 2014

[3] 조미영, 김기천, “NFC 시장 현황 및 활성화 방안 연구”, 한국통신학회지(정보와통신), 29(6), pp. 58-66, 2012.5

[4] “2012년 하반기 스마트폰 이용실태조사 요약보고서” 한국인터넷진흥원, 2013

[5] Google Play, 키워드 “nfc tagInfo”, 2018.11

[6] Google Play, 키워드 “NFC reader and writer - NFC Tag Reader Tools”, 2018.11

[7] Google Play, 키워드 “NFC Tag Tools”, 2018.11

[8] Google Play, 키워드 “NFC Reader Pro“, 2018.11

[9] Google Play, 키워드 ”NFC Reader&Writer“, 2018.11

[10] Google Play, 키워드 ”nfctools“, 2018.11

[11] onnfc, 한글nfcwriter by onnfc, 2018.11, “http://www.onnfc.com/”

[12] nfctouch+, “https://www.nfctouch.com.hk/”, 2018.11

[13] Google play, 키워드 “korea nfc writer”, 2018.11

[14] 장은겸, ″NFC를 사용한 명함 전송 및 제작 어플리케이션″, 한국컴퓨터정보학회 학술발표논문집, 24(1), pp. 195-196, 2016.1

[15] 조대수, ″NFC를 활용한 출결관리 시스템 구현″, 한국정보통신학회논문지, 17(7), pp. 1639-1644, 2013.07

[16] 강기범, 좌정우, 김순환, 김홍수 “NFC 기술을 이용한 카드 분실을 방지하기 위한 모바일 앱”, 한국전자통신학회 논문지, 12(1), pp. 181-187, 2017

[17] 오용택, 천유정, 최순영, Scoot UK-jin Lee ″스마트폰의 NFC를 사용하는 스마트 아파트 서비스 관리 시스템″, 한국정보과학회 학술발표논문집, pp. 1393-1395, 2016.12

[18] 김은주, 정다훈, 황세연, 지정희 ″NFC 통신을 이용한 IoT 도어락 모듈 및 어플리케이션 IMLOCK″, 한국통신학회 학술대회논문집, pp. 779-780, 2017.6

[19] 최정원, 유현주, 정민수 ″NFC를 활용한 개인 정보 보호 택배 서비스 안드로이드 어플리케이션 설계″, 한국정보과학회 학술발표논문집, pp. 1384-1386, 2013.11

[20] 행정안전부 정보기반보호정책과, “공공웹사이트 인증수단 소개서”, 2018.9.

[21] 김성윤, 유현주, 정민수 ″NFC서비스모델을 통한 NFC활성화 방안 연구″, 한국통신학회 학술대회논문집, pp. 98-99, 2012.2

[22] 김수철, 여상수, 김성권 “RFID 프라이버시 보호를 위한 향상된 모바일 에이전트 기법”, 한국통신학회 논문지, 33(2), pp. 208-218, 2008.02