AIDA : NFC를 이용한 IoT 기반 출입통제 앱

윤혜민, 김연정, 박주희, 이지혜, 채서연, 김명주
서울여자대학교 정보보호학과
e-mail:hyemin3307@naver.com

AIDA: a Mobile Application for IoT-based Doorlock using NFC

HyeMin Yun, YeonJeong Kim, JooHee Park , JiHye Lee, SeoYeon Chae, Myuhng Joo Kim
Dept of Information Security, Seoul Women's University

요 약

본 연구는 교내 카드 학생증의 불편함을 해소하기 위해 무선통신 NFC 기술을 활용하여 IoT 도어락을 구현했다. 본 앱의 목적인 출입과 동시에 권한 양도 기능을 수행함으로써 교내 이외 실생활에서도 적용가능 하도록 구현하였으며, 이를 통해 편리성, 효율성, 보안성을 모두 갖출 수 있도록 구현했다.

1. 서론

대학 내 건물들은 일반적으로 학생증 신분카드로만 출입이 가능하기 때문에 학생증 카드 미소지 시 학생들이나 교직원들은 본인에게 합법적인 출입권한이 있음에도 불구하고 불편함을 많이 느끼고 있다. 본 연구에서는 신분카드 뿐 아니라 모바일 앱을 이용해서도 열 수 있는 IoT 도어락을 제작하였고, 더불어 외부인 출입 보안도 강화하고 학생증 대시할 수 있도록 하여 출입의 편리성을 제공하고자 한다.

NFC는 P2P 접속방식을 사용하며 필요할 때마다 자체적으로 태그 역할과 태그 정보를 읽거나 쓰는 역할도 할 수 있다. 무선통신 방식이기 때문에 편리하지만 연결해야하는 단말기가 4~10cm 이내에 존재하여야 식별될 수 있다는 제한점이 있다[1]. 그러나 이러한 제한점이 출입에 있어서는 장점이 될 수 있어서 NFC를 이용한 IoT 도어락을 시도하였다.

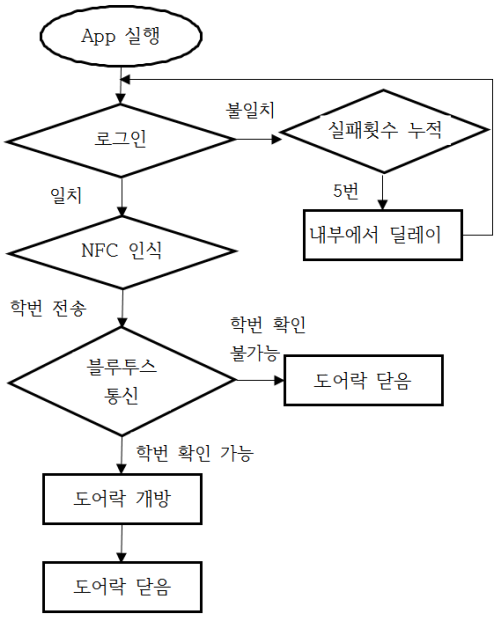
이 IoT 도어락과 통신해서 건물을 출입하는 모바일 앱을 제작하였고 해당 앱의 이름은 AIDA이다. A는 Authentication, I는 Integrity, DA는 Delegation of Authority로 '본인 인증 후에 출입을 하며 인가되지 않은 방법으로는 출입할 수 없도록 보호하고 권한을 양도할 수 있다'라는 의미를 담고 있다. 또한 한글로 '아이다'라고 해서 '아무나 들이지 않는다'의 줄임말이기도 하다.

AIDA 앱의 주요 기능 중 하나인 '권한 양도'는 학교 내에서 사용하는 상황에만 머물러 있지 않고, 실생활에서도 권한 위임이 필요한 시점에 사용할 수 있다. 또한 편리성 뿐 아니라 보안성을 높이기 위해 2차 비밀번호 등 여러 가지 기술을 포함하였다.

본 논문에서는 편리성과 보안성을 갖춘 IoT 도어락과 앱을 제작하는데 있어서 앱의 작동 과정, 출입 기능, 보안 기능, 서버 및 데이터베이스 통신원리, 아두이노 작동과정에 대해 설명한다.

2. 본론

2.1 작동 프로세스 및 서버



<그림 1> AIDA 작동 알고리즘

<그림 1>은 전체 작동 과정 알고리즘이다. 앱을 실행하면 바로 로그인 화면이 뜬다. 이 때 학번과 비밀번호를 입력하여 로그인하는데, 일치하는 경우 문제없이 다음 단계로 넘어가지만, 일치하지 않는 경우 실패 횟수가 누적 된다. 횟수가 5번이 되면 다시 로그인을 시도하기 전까지 시간을 제한하여 내부에서 딜레이 시킨다. 일치하면 NFC 인식으로 도어락과 통신하고 아이디로 사용한 학번을 블루투스 통신을 통해 아두이노로 전달하여 이더넷 통신을 통해 서버로 HTTP 요청을 전송한다. 서버가 '학번 확인 가능' 응답을 보내면 도어락을 개방하고, '학번 확인 불가능' 응답을 보내면 도어락을 열지 않는다.

앞서 앱 작동과정에서 사용된 서버는 PHP, Mysql을 이용하여 구축하였다. PHP의 HTTP 요청에 따라 Mysql 데이터베이스에 저장하거나 혹은 결과값을 반환하여 비교한다.

<표 1> 앱 사용자에 따른 출입권한 분류

	앱 사용 유형	출입권한
A	계정이 있는 사람	O
B	계정이 없지만 권한 양도를 받은 사람	△
C	계정이 없지만 권한 양도를 받지 않은 사람	X

서버가 필요한 가장 큰 이유는 출입권한이 있는 사람인지 아닌지 판단하기 위함이다. O는 권한이 있는 사람, X는 권한이 없는 사람, △는 일차적으로 권한이 없으나 일시적으로 허가받을 수 있는 사람이다. 일차적으로 로그인 시 계정이 있다면 권한이 있는 사람(A)으로 판단한다. 계정이 확인된 사람들은 출입에 대한 권한을 모두 부여받으며, 자신의 출입 기록을 확인 및 권한 양도 관리 등이 가능하다. 이차적으로 계정이 없는 사람들 중 권한 양도를 받은 사람(B)이라면 출입권한을 일시적으로 허가해야하기 때문에 서버에 권한을 받는 사람의 정보를 저장하여 확인한다. 이외에 계정이 없지만 권한 양도를 받지 않은 사람(C)은 출입에 어떠한 권한도 부여받지 않는다. 그리고 이 모든 과정은 서버를 통해서 이루어진다.

2.2 출입 기능

[그림 2]는 도어락 시스템 구성도이다. 시스템은 출입을 위한 메인 앱, 전면 도어락, 후면 도어락으로

<그림 2> 도어락 시스템 구성도

구성되었으며, 전면 도어락은 NFC 통신과 블루투스 통신을 위해 서브 앱과 아두이노를 이용하였다.

학교 종합정보시스템에 등록된 계정으로 메인 앱에 로그인 할 수 있다. ① 로그인에 성공 시 출입권한을 위한 NFC Tag가 생성되며, 이 때 생성된 Tag를 서브 앱으로, ② 서브 앱에서 다시 아두이노로 전송한다. ③ 아두이노는 서브 앱에서 받은 값으로 서버에 HTTP 요청을 보낸다. ④ 서버가 '학번 확인 가능' 응답을 보내면 도어락을 개방하고, '학번 확인 불가능' 응답을 보내면 도어락을 열지 않는다. ④번까지 완료되면 종합정보시스템에 등록된 계정 소유자는 건물 출입이 가능하다.

출입 시스템을 수행하는 데에 있어 기존보다 효율성과 보안성을 향상시키기 위해 권한 양도 및 외부인 일회성 출입권한 부여 기능을 추가했다. 주요 기능 중 하나인 권한 양도에는 외부인 권한 양도, 권한 양도 관리, 내부인 간의 권한 부여로 구현했다. 여기서 외부인은 기존에 출입 권한이 없는 자이며, 내부인은 출입 권한을 소유하고 있는 자이다. 먼저 외부인 권한 양도는 권한을 받는 자(외부인)가 권한을 주는 자(내부인)에게 권한 양도를 요청할 때 사용한다.

이를 수행하기 위해서는 권한을 받는 자(외부인)가 먼저 본인의 핸드폰 번호를 입력 후 SMS 인증을 수행하게 된다. 인증이 성공하면 권한을 주는 자(내부인)의 핸드폰 번호와 출입목적을 직접 작성하여 권한을 주는 자(내부인)에게 SMS 인증을 보내 인증을 수행하게 된다. 권한을 주는 자(내부인) 역시 인증에 성공하게 되면 권한 부여에 성공하며, 이 때 출입을 위한 인증키가 생성되고 데이터베이스에 저장된다. 이 후 도어락 오픈 시 NFC로 넘어간 학번이나 핸드폰 번호가 Database에 저장된 데이터인지 확인을 위해 서버로 Http Request를 보내게 된다. 권한을 받는 자(외부인)의 권한을 끊기 위해서는 본인이 직접 '출입권한 반납하기' 기능을 수행해야 하

며, 이를 불이행 시 다른 사람에게 양도 받을 권한이 제한되며, 권한을 주는 자(내부인)가 강제적으로 반납을 수행한다.

권한 양도 관리 및 새로운 권한은 권한 소유자가 로그인 후 사용가능한 메뉴로써 권한 소유자가 권한을 양도 한 일시, 목적을 확인할 수 있고, 어떤 곳을 출입했는지 확인할 수 있으며, 학교 출입 시 외부인 출입을 재제하고, 직접 출입 관리를 함으로써 보안성이 크게 강화된다는 것을 알 수 있다.

마지막으로 내부인 간의 권한 부여는 권한을 소유하고 있는 자 중에서도 학교 내의 역할 및 직책에 따라 출입의 권한이 제한 된 곳에 사용된다. 교내 인턴 및 조교, 교수 등 역할을 대신하여 임무를 수행할 수 있는 상황이 간혹 발생하게 되었을 때, 수행하게 되는 기능이다. 권한을 부여받는 절차는 앞서 외부인 권한 양도 절차와 비슷한데 외부인과의 차이점은 권한을 받는 자, 권한을 주는 자 모두 기존에 권한을 소유하고 있는 자로써 데이터베이스에 정보가 저장되어있다. 그러므로 권한을 받는 자의 핸드폰 번호 인증 절차를 생략하고, 권한을 주는 자의 핸드폰 번호와 목적을 기입하여 권한을 양도받을 수 있도록 구현했다.

2.3 보안 기능

우선 로그인 횟수를 5번으로 제한했다. 아이디와 비밀번호의 오류가 5번으로 비정상 로그인 시도가 되면 30초 동안 앱이 잠기게 된다. 이후로는 1분, 2분으로 계속 늘어나게 된다.

1계정 1기기 등록으로 핸드폰 분실 시에 대한 대안을 마련했다. 기기등록해제는 한 달에 두 번으로 횟수가 제한된다. 또한, 학생증 카드 분실 시 구축한 데이터베이스를 이용해 앱에서도 카드 사용정지를 할 수 있도록 하여 빠르게 보안대응을 할 수 있다. 또한, 핸드폰 분실 시 추가로 PIN 번호와 지문인증과 같은 2차 비밀번호를 통해 보안을 한 단계 더 강화했다. 비밀번호 활성화/비활성화 및 변경 또한 가능하다.

권한을 받는 자(외부인)의 본인인증과 권한을 주는 자(내부인)의 권한 양도 승낙 및 거부는 SMS를 통한 본인인증과 인증키 생성 및 데이터베이스 삽입을 통해 권한 양도에 대한 보안성을 높였다.

데이터베이스에 입력된 정보를 이용하여 권한 양도 및 외부인 출입 기록을 볼 수 있어 출입에 대한 보안성을 강화했다. 권한을 양도한 사람이 본인에게 누구에게, 어떤 사유로 권한을 양도했는지 보여준다. 외부인 출입 일시와 출입 사유를 보여준다.

앱을 이용하기 위해서는 학교 시스템에 등록된 계정을 이용한다. 따라서 수집하는 개인정보는 학교에서 기재되는 기본 개인정보 처리 방침을 따른다. 학교 건물을 출입하는 사람들은 다양하기 때문에 사유를 분류하여 수집하는 개인정보 항목을 나누었다. 개인정보의 파기절차 및 방법 또한 학교에서 기재되는 기본 방법을 따랐다.

3. 결론

개발 결과 학생증이 없어도 학교 건물을 편하게 출입 할 수 있어 사용자의 편리성 증대를 기대할 수 있고, 보안적인 요소를 더하여 출입 보안을 강화하였다.

NFC 태그와 권한 양도기능은 일상의 다양한 상황과 광범위한 장소에서 활용될 수 있다. NFC 태그를 대형 강의나 지정 좌석 출석에 활용하여 편리성을 증대할 수 있다. 또한, 공연좌석에 NFC 태그를 활용한 결제시스템을 도입하면 인터넷이나 현장구매로 줄을 서지 않고 본인이 원하는 좌석에 앉아 그 자리에 결제할 수 있다.

택배기사에게 매번 비밀번호를 전해야 하는 번거로움을 권한 양도기능을 통해 해결할 수 있다. 본인의 택배 함을 여는 권한을 양도한다면 빠르고 안전하게 택배 함을 열 수 있다. 이는 아마존의 택배서비스에서 도입하려는 주인 없는 집 안에 택배물건 배달 서비스보다 더 간단한 서비스라고 할 수 있다[2]. 또한, 아파트 외부인이 주차장을 이용해야 하는 상황에도 적용할 수 있다. 주민이 직접 외부인에게 주차 권한을 준다면 외부인 주차문제를 해결할 수 있을 것이다.

이렇게 NFC와 권한 양도의 기능은 일상생활에서 다양하게 쓰일 수 있다. 따라서 권한 양도를 포함해 다양한 기능을 갖는 AIDA 앱은 다양한 상황에 접목할 수 있어 앱 상용화 및 발전성을 보여준다.

참고문헌

[1] 세종트로닉스, “NFC 장점”, http://www.sejongtns.com/ProductMD_NFC_02.html , (2018.03.17.)

[2] http://news.donga.com/3/all/20171027/86977576/1