주거침입 범죄 예방을 위한 스마트 도어락 시스템 설계와 구현

강현민, 박서현, 차경애
대구대학교 정보통신공학부 멀티미디어공학전공
e-mail:kanghyeonmin@gmail.com

Smart Door Lock System Design for Housing Crime Prevention

Hyeon-Min Kang, Seo-Hyeon Park, Kyung-Ae Cha
Daegu University

요 약

본 설계의 목적은 디지털 도어락의 아웃바디를 파손하여 침입하는 1차원적인 외부침입자를 차단하기 위한 것이다. 일반적인 디지털 도어락은 아웃바디와 인바디가 케이블로 연결되어 도어락을 제어하는 구조로 설계되어 있으므로, 아웃바디를 파손하면 인바디의 제어기능이 손상된다. 따라서, 본 논문에서는 아웃바디와 인바디를 독립적으로 배치하고 상호간의 무선 통신을 통하여 도어락을 제어하도록 설계하였다. 이것은 아웃바디를 파손하여도 인바디의 기능이 손상되지 않도록 하기 위함이다. 그 결과, 도어락의 아웃바디를 파손하여도 침입이 불가능한 구조의 스마트 도어락을 구현할 수 있었다.

1. 서론

최근 사회의 가족형태 중 가장 큰 변화는 하나는 1인 가구가 증가하고 있는 현상이다. 학업, 직장 등 다양한 이유를 바탕으로 1인가구의 수는 꾸준히 증가하고 있으며 그 중 한국은 OECD국가 중 가장 빠른 1인 가구 증가세를 보이고 있다. 2010년도 주거침입 피해 대상자의 31.2%가 1인가구인 것으로 파악되어 이들이 범죄피해에 가장 크게 노출되어 있음을 알 수 있으며, 이들을 대상으로 한 범죄율 또한 꾸준히 증가하고 있으므로 1인가구에 거주하는 많은 사람들이 범죄에 대한 걱정을 가지고 있다[1]. ADT 캡스의 2016년 자사의 출동 데이터를 분석한 '2016년 범죄동향'에 따르면 도둑의 침입 경로는 출입문을 통한 침입이 38.1%로 가장 높았으며 이는 접근이 쉬운 출입문을 노린 형태가 많다는 것을 의미한다[2].

도어락이란 가장 대표적인 안전장치로써 침입자로부터 집을 안전하게 보호하기 위해서는 보안을 강화하는 것이 필수적으로 요구된다[3]. 디지털 도어락 시장에서는 생체인식, 음성인식 등 다양한 기술을 이용하여 보안을 강화하기 위해 힘을 쓰고 있으며, 무선통신을 이용한 도어락 관련연구는 인바디와 아웃바디 간의 연결이 아닌 스마트폰과 도어락의 연결을 주제로 진행되고 있다. 따라서, 도어락 아웃바디를 파손 하여 침입하는 1차적인 외부침입자를 차단하는 것은 어려운 실정이며 정확한 인식이 되지 않는 등 다양한 문제를 발생시키고 있다.

본 논문에서는 일상에서 자주 사용되는 디지털 도어락을 블루투스(Bluetooth)와 FCM(Firebase Cloud Message)를 이용하여 아웃바디를 파손하여도 침입이 불가능한 구조의 도어락을 설계한다. 이를 위해서 아웃바디와 인바디가 케이블로 연결되어 작동하는 일반적인 도어락과 달리, 인바디와 아웃바디를 독립적으로 배치하고 상호 간의 블루투스 통신을 통하여 작동하도록 설계하였다. 또한, 도어락이 제어될 시 사용자에게 푸시메시지를 전송하고 제어 내역을 저장함으로써 보다 체계적인 출입내역 관리 등의 서비스를 제공한다.

2장에서는 사용된 기술을 소개하며 3장에서는 본 논문의 무선 통신을 이용하여 주거침입 범죄 예방을 위한 스마트 도어락의 설계 및 구현 내용을 설명한다. 4장에서는 구현한 시스템의 결과를 보이고 5장에서는 결론을 제시한다.

2. 사용된 기술

2.1 블루투스 기술

블루투스(Bluetooth)는 특정 기기를 서로 연결해 정보를 교환하는 무선 기술 표준을 뜻하며 초단거리에서 저전력 무선 연결이 필요할 때 사용된다.

2.2 푸쉬 알림 서비스(Push Alarm Service)

푸쉬 서비스는 사용자의 요청이 없어도 서버를 통해 메시지를 사용자 디바이스에 제공할 수 있는 서비스이다[4]. 과거의 SMS(short message service) 또는 MMS (multimedia message service)는 비용이 발생하는 것과 달리 푸쉬 메시지는 부과 비용이 없으며, 서버를 통하여 메시지를 특정 스마트폰 어플리케이션으로 전송할 수 있

다. 이러한 푸쉬 메시지를 제공하는 대표적인 서비스는 FCM(Fire Base Messageing)이 있다[5,6].

3. 무선통신을 이용한 도어락 제어

3.1 시스템 동작 개념

본 논문에서 제안한 무선통신을 이용한 도어락 제어 시스템은 케이블을 통한 데이터 통신 대신, 블루투스를 이용하여 도어락을 제어한다.

이 시스템의 전체 구조는 그림 1과 같이 도어락의 아웃바디, 인바디, FCM을 구현하는 푸쉬서버 및 스마트폰 어플리케이션으로 구성된다.

불특정 사용자는 도어락의 아웃바디에서 비밀번호를 입력한다. 이 때, 인바디는 입력된 비밀번호를 블루투스 통신을 통하여 전송받고 등록된 비밀번호와 일치할 경우 도어락을 제어한다.

(그림 1) System Operation Concept.

불특정 사용자는 스마트폰 어플리케이션으로도 도어락을 제어할 수 있으며, 도어락이 제어되었을 경우 사용자의 스마트폰으로 제어 알림 메시지가 전송된다. 이러한 구조를 통하여 아웃바디가 파손되어도 인바디의 기능손상이 일어나지 않아, 아웃바디 파손을 통한 침입이 불가능하며, 도어락 제어내역의 기록과 관리가 이루어져 보다 안전성이 뛰어난 도어락의 구현이 가능하다.

3.2 시스템 설계 및 구현

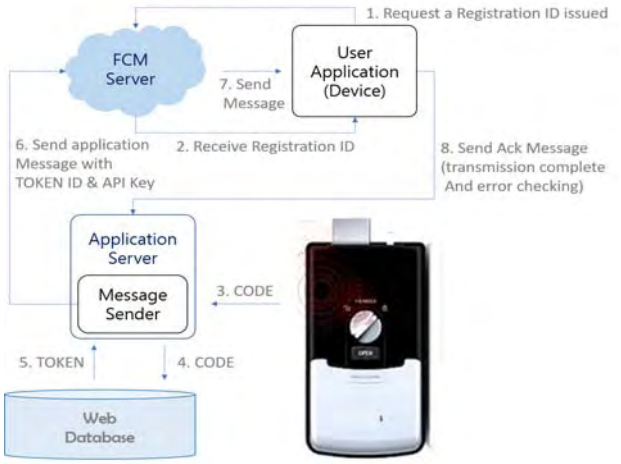
3.2.1 FCM 서비스 구현

FCM 푸쉬 메시지 서비스를 활용하기 위해서 FCM API를 이용해 서비스를 구현한다. 도어락 제품마다 고유코드가 있으며 불특정인은 제공된 코드를 이용하여, 푸시 메시지를 수신 받을 스마트폰 단말기를 등록한다. 이 때, 사용자 정보는 그림 2와 같이 웹 데이터베이스에 저장된다.

CODE	ID	PASSWORD	TOKEN
A4509DNO	HYEONMIN	PASSWORD	APA91bEWqSXsG4khW8A3Fnnxj-q-jMF6X9kQeww_IOmqenG_K2
C420X9M3			
ZY53X97W			

(그림 2) Web Database.

그림 3은 제안한 도어락 시스템의 푸쉬서버와의 동작 구조이다.

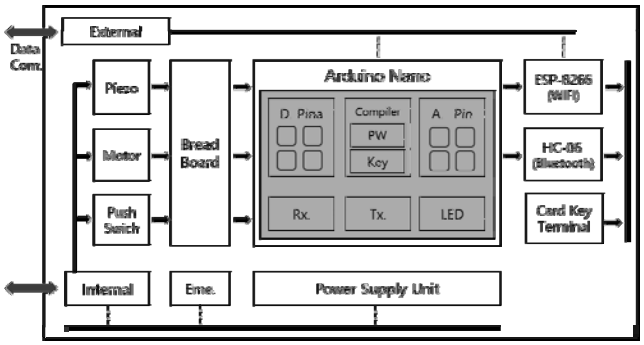


(그림 3) FCM Push Message Service Process.

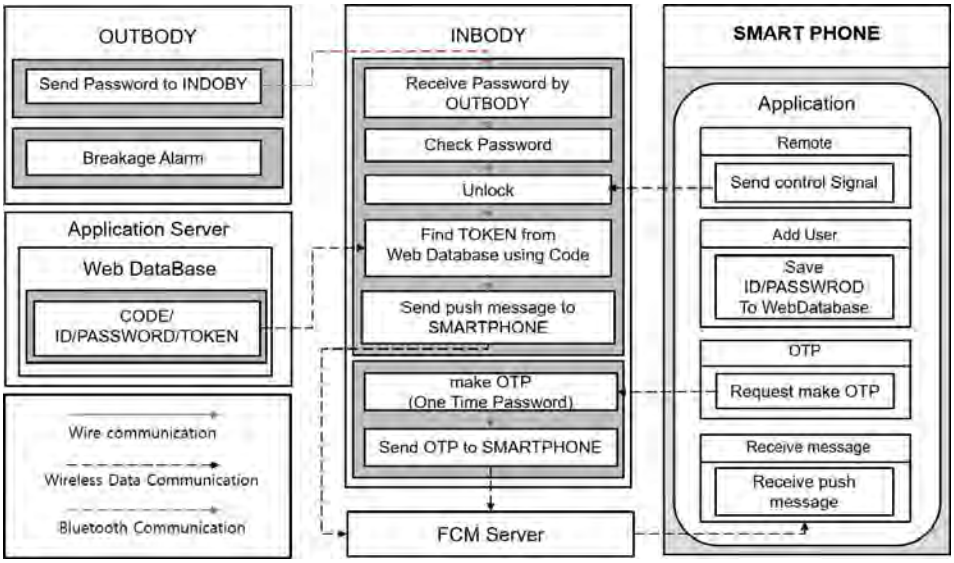
웹 데이터베이스에 사용자 등록이 완료된 후(그림 3의 1-2) 도어락이 제어되면, 인바디는 어플리케이션 서버로 제품 고유코드를 전송하고(그림 3의 3), 어플리케이션 서버는 고유코드에 매칭되는 사용자의 토큰값을 받아온다(그림 3의 4-5). 받아온 토큰값은 FCM 서버로 전달되며(그림 3의 6), FCM 서버는 토큰값에 매칭되는 사용자의 단말기로 메시지를 전송한다(그림 3의 7). 사용자 단말기는 FCM서버로부터 메시지가 수신되면, 사용자에게 메시지가 전달되었음을 알리고, 어플리케이션 서버에 확인 메시지를 전송한다(그림 3의 8).

3.2.2 도어락 인바디 및 아웃바디 구현

인바디의 전체적인 블록 다이어그램은 그림 4와 같다. 기본적인 MCU에 해당하는 아두이노 나노를 중심으로 하여 브래드보드에 부저, 모터, 푸쉬 스위치가 연결되어 있으며, 와이파이 통신 모듈인 ESP-8266와 블루투스 모듈 HC-06, 카드키 단말기가 아두이노 나노와 연결되어 있다. 이는 하나의 보드로 제작되어 인바디 내부에 결합되어 있으며, 이와 직접적으로 연결된 것이 배터리와 예비 전원이다.



(그림 4) InBody Block Diagram



(그림 5) System Structure.

인바디는 전원이 연결되면 블루투스 모듈인 HC-06 Master/Slave 통신으로 Master로 고정되어 Slave로 설정된 아웃바디와 자동 페어링된다. 또한 ESP-8266 모듈은 사용자가 설정한 무선 네트워크와 연결된다.

아웃바디의 경우 그림 4와 같이 MCU를 사용하나, 다른 모듈은 사용하지 않고 HC-06모듈을 이용한 블루투스 통신만을 하게 된다. 앞서 설명한 것과 같이, 아웃바디는 Slave로써 Master에 데이터를 전송한다.

3.2.3 어플리케이션 설계 및 구현

제안한 시스템의 구현을 위해, 스마트폰에서 사용되는 어플리케이션과 FCM 서버 및 어플리케이션 서버를 그림 5와 같이 설계하였다. 앞서 설명한 FCM 서비스의 푸쉬 메시지를 활용하기 위해서는 디바이스 식별과 웹 데이터베이스에 저장되는 TOKEN값을 관리할 수 있는 어플리케이션 서버를 구현하여야 한다. 어플리케이션 서버는 아이디를 사용하여 해당 아이디에 등록된 스마트폰의 TOKEN값을 검색하는 기능을 담당한다.

스마트폰에 탑재되는 어플리케이션은 도어락의 사용자를 등록하는 기능과, 인바디로 제어 신호를 전송하는 기능을 구현한다. 또한, 푸쉬 메시지가 수신되면 수신된 메시지의 정보를 내부 데이터베이스에 저장한다.

4. 구현 및 실험 결과

제안한 도어락의 구현을 위해 아두이노 나노(Arduino nano), 와이파이 모듈(ESP 8266), 블루투스 모듈(HC-06), 서브 모터(Servo Motor)을 사용하였으며, 어플리케이션의 개발을 위해 윈도우즈 개발환경에서 ADT(Android Develop Tool)을 사용하였다. 어플리케이션 서버 구현에는 NAS서버와 PHP, MYSQL을 사용하였으며, 푸쉬 서버 기능 구현을 위해서 FCM API를 이용하였다.

그림 6는 구현한 어플리케이션의 화면이다. 버튼 클릭만으로 간단하게 도어락을 제어할 수 있도록 구현하였으며, 아웃바디 또는 스마트폰을 통하여 도어락이 제어되면 사용자의 스마트폰으로 푸시 메시지가 전송되고, 제어 내역은 내부 데이터베이스에 저장된다.

(그림 6) Application Layout.

표 1은 주거침입 범죄를 예방하기 위한 기존의 방법들과 본 시스템과의 비교 분석 내용이다. 본 논문에서 구현한 시스템은 기존 제품들이 다양한 센서들을 이용하여 보안을 강화하는 것과 달리, 통신방법의 전환을 통하여 보안을 강화하여 파손 침입에 대한 대비책을 제시한다.

<표 1> Comparsion of other security methods and proposed systems

	Fingerprint Recognition	Iris Recognition	Bluetooth
Cost	average	expensive	cheap
Safety	average	dangerous	safe
accuracy	accurate	inaccurate	avarage

5. 결론

1인가구가 증가함에 따라 이들을 대상으로한 주거침입 범죄율이 계속 증가하고 있으며, 이에 따라 방범장치 등 주거안전에 대한 제품이 관심을 받고 있다. 본 논문에서 제안한 시스템은 방범장치 중 가장 대표적인 디지털 도어락 시스템으로써 기존의 도어락 파손 침입에 대한 해결책을 제시하여 주거침입에 대한 불안감을 해소한다. 또한, 도어락의 인바디가 실내 네트워크에 연결되어 원격 제어, 제어 알림 서비스, OTP(One Time Password) 등 다양한 스마트 기능을 제공한다. 향후 실제 활용하고 검증을 통해서 보완 내용을 수집하고 조금 더 편리한 서비스를 제공하기 위하여 꾸준히 개발할 예정이다.

참고문헌

[1] E.H. Oh, "Regional Crime Prevention Service APP Design for Single Households", *Korea Society of Design Trand*, Vol. 50, pp. 65, 2016.

[2] Crime Trends in 2016 ADT Caps Employment. http://adtcaps.co.kr (accessed Jun., 13, 2017).

[3] Y.L. Cho, Y.G. Kim, J.H Shim, J.H Lee, E.H. Chol, D.H Lee et al. "Design of Secure and Convenient Smart Door Lock System based on OTP in IoT Environment", *Korean Institute of Information Scientists and Engineers*, Vol. 2016, No. 6, pp. 1817, 2016.

[4] Hyun-Min Kang, Hyun-Su Choi, Kyung-Ae Cha, "Development of Vehicle Status Alerts System for Personal Information Leakage Protection using the NFC-based GCM Service", *Journal of Korea Multimedia Society*, Vol. 2016, No. 2, pp. 317, 2016.

[5] GCM(Google Cloud Messaging) for Android, http://leminity.tistory.com/26 (accessed Sept.,22, 2015)

[6] C.H. Jung, J.H. Ye, and C.J. Kim, "A Mobile Customization Technique using Push Service", *Journal of the Korea AcademiaIndustrial Cooperation Society*, Vol. 14, No.9, pp. 4498-4506, 2013.