보안기능이 강화된 디지털 도어락 설계 및 구현

허동혁 [1], 신상호 [2], 정기현 [1, *]
경일대학교 사이버보안학과 [1], 경주 스마트미디어센터 [2]
e-mail : hdh990526@naver.com, shshin.study@gamil.com, khanny.jung@gmail.com

Design and Implementation of Digital Door Lock for Robust Security

Dong-Hyeok Heo, Sang-Ho Shin, Ki-Hyun Jung
Department of Cyber Security, Kyungil University, Korea
Division of Technology Development, Gyeongju Smart Media Center, Korea

요 약

IoT 환경에서 디지털 도어락에 대한 관심과 사용이 증대되고 있다. 이러한 디지털 도어락의 사용 증가와 해킹 공격으로 인한 정보 유출이 지속적으로 발생하고 있는 현실 상황에서 보안 문제도 중요하게 대두되고 있다. 본 논문에서는 보안 문제를 해결하기 위한 디지털 도어락을 설계하고 구현하였다. 제안된 시스템을 통하여 보안 취약점을 보완하고 편의성을 제공 가능할 것으로 기대된다.

1. 서론

IoT 보안 중 가장 중요한 사항 중 한 가지는 인증 기능으로 IoT 기기 중 인증처리가 중요한 디바이스로 디지털 도어락이 대표적이다. 이러한 디지털 도어락은 기존 키를 사용하는 아날로그 도어락을 점점 대체하고 있는 추세이다. 디지털 도어락은 기본적으로 보안 취약성이 적어야 하는데, 최근 이중 잠금, 스마트폰 앱 연동을 통한 인증 카드키 사용 등 인증이 강화된 보안 기능을 탑재한 제품들이 출시되고 있다 [1-2].

이러한 다양한 보안 기능을 제공하는 디지털 도어락이 사용되고 있음에도 불구하고, 고도화된 보안 취약성 공격을 통하여 디지털 도어락의 인증 체계가 뚫리고 있는 상황으로 이와 연계된 피해도 점점 증가하고 있다. 이런 해킹 공격이 발생하는 이유로는 사용자가 매뉴얼을 통하여 디지털 도어락의 보안기능을 제대로 설정하지 않은 경우와 공격자가 기존의 보안 취약점을 통하여 디지털 도어락의 보안 기능을 무력화시키는 경우로 크게 나눌 수 있다 [10-12].

본 논문에서는 기존 디지털 도어락의 취약점을 분석하고, 보안 취약점을 보완할 수 있는 시스템을 설계하고 구현한다. 또한, 일반 사용자도 쉽게 사용할 수 있도록 보안 기능의 편리성과 접근성을 향상시킬 수 있도록 제공한다.

2. 관련 연구

2.1 디지털 도어락

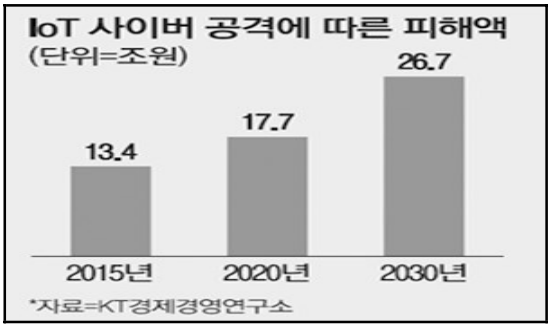
지금까지도 열쇠를 이용하는 아날로그 도어락이 많이 사용되고 있으나, 디지털 도어락에서 제공하는 편리성과 보안성으로 디지털 도어락 사용이 증가하고 있는 추세이다.

디지털 도어락의 보안기능을 살펴보면, <표 1>과 같이 이중 잠금, 허수 기능, 패스워드, 앱 연동 등의 기능들이 많이 사용되고 있다 [3-5].

<표 1> 디지털 도어락 보안기능

보안 기능	효과
이중 잠금	내부에서 열림 버튼이 활성화되지 않음
허수 기능	패스워드를 입력하고도 다른 번호를 입력하여 도청 중인 공격자에게 혼란을 주거나 지문 채취를 방지할 수 있음
패스워드	알맞은 패스워드를 입력해야 디지털 도어락이 열림
전용 앱 통신	스마트폰 앱과 연동하여 출입내역 원격 조종 등을 통하여 디지털 도어락을 제어할 수 있음

다음으로 디지털 도어락을 포함한 IoT 사이버공격 피해액을 살펴보면 (그림 1)과 같으며, 그 피해액이 점점 증가하고 있음을 알 수 있다 [6].



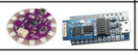
(그림 1) 사이버 공격 피해 현황

* 교신저자: Ki-Hyun Jung (Tel. +82-53-600-5626, E-mail. khanny.jung@gmail.com)

2.2 아두이노와 라즈베리 파이

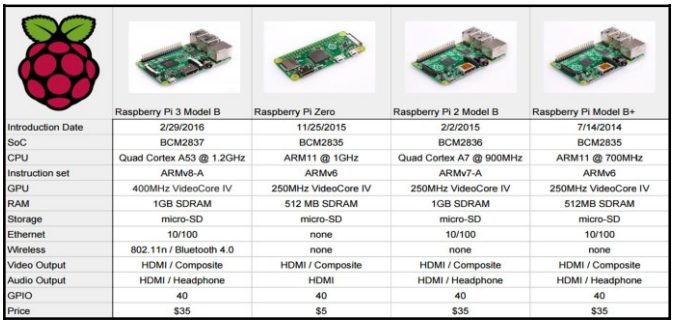
아두이노는 간단한 통신을 통하여 반복적인 동작을 수행하게 하는 하드웨어로 다양한 모듈을 활용하여 본 논문에서 제안한 시스템을 효율적으로 구현할 수 있다. 현재 <표 2>에서 보는 바와 같이 다양한 모델을 제공하고 있으며, 아두이노 UNO 가 일반적인 모델이다. 아두이노 Mega2560 의 경우에는 다양한 단자를 제공하고 있어 많은 모듈들을 장착할 수 있는 장점이 있다 [7].

<표 2> 아두이노 모델과 스펙

Name	Picture	Processor	Operating Voltage/ Input Voltage	SRAM [KB]	Flash [KB]	USB	UART
UNO		ATmega328	5 V/7-12 V	2	32	Regular	1
DUE		AT91SAM3X8E	3.3 V/7-12 V	96	512	2 Micro	4
Leonardo		ATmega32u4	5 V/7-12 V	2.5	32	Micro	1
Mega2560		ATmega2560	5 V/7-12 V	8	256	Regular	4
Micro		ATmega32u4	5 V/7-12 V	2.5	32	Micro	1
Mini		ATmega328	5 V/7-9 V	2	32	–	–
Nano		ATmega168 ATmega328	5 V/7-9 V	1 2	16 32	Mini-B	1
Pro Mini		ATmega168	3.3 V/3.35-12 V 5 V/5-12 V	1	16	–	1
LilyPad		ATmega168V ATmega328V	2.7-5.5 V/2.7-5.5 V	1	16	–	–
LilyPad USB CactusMicro		ATmega32u4	3.3 V/3.8-5V	2.5	32	Micro	–

본 시스템에서는 아두이노 UNO 와 Mega2560 두 가지 모델을 사용하여 시스템을 구현하고 있다.

라즈베리 파이는 소형 컴퓨터 역할을 해주는 하드웨어로 우분투, 라즈비안 등의 운영체제를 사용할 수 있다. 라즈베리 파이의 경우 아두이노와 연결하여 시리얼 통신 기능을 수행하는 것도 가능하여 이를 사용하여 라즈베리 파이를 아두이노와 신호를 주고받으며 중앙통제 역할로 사용하는 등의 활용이 가능하다.



	Raspberry Pi 3 Model B	Raspberry Pi Zero	Raspberry Pi 2 Model B	Raspberry Pi Model B+
Introduction Date	2/29/2016	11/25/2015	2/2/2015	7/14/2014
SoC	BCM2837	BCM2835	BCM2836	BCM2835
CPU	Quad Cortex A53 @ 1.2GHz	ARM11 @ 1GHz	Quad Cortex A7 @ 900MHz	ARM11 @ 700MHz
Instruction set	ARMv8-A	ARMv6	ARMv7-A	ARMv6
GPU	400MHz VideoCore IV	250MHz VideoCore IV	250MHz VideoCore IV	250MHz VideoCore IV
RAM	1GB SDRAM	512 MB SDRAM	1GB SDRAM	512MB SDRAM
Storage	micro-SD	micro-SD	micro-SD	micro-SD
Ethernet	10/100	none	10/100	10/100
Wireless	802.11n / Bluetooth 4.0	none	none	none
Video Output	HDMI / Composite	HDMI / Composite	HDMI / Composite	HDMI / Composite
Audio Output	HDMI / Headphone	HDMI	HDMI / Headphone	HDMI / Headphone
GPIO	40	40	40	40
Price	$35	$5	$35	$35

(그림 2) 라즈베리 파이 분류

(그림 2)에서와 같이 다양한 제품이 출시되고 있으며, 가장 보편적인 모델은 Raspberry Pi 3 B+이라고 할 수 있다. Raspberry Pi 3 B+는 CPU 가 1.2GHz 에서 1.4GHz 로 상향되었으며 와이파이 모듈 교체와 함께 블루투스 모듈이 4.1 에서 4.2 버전까지 지원 가능하게 되었다 [8].

2.3 OTP

OTP(One Time Password)는 한번 사용되고 나면 사라지는 일회성 비밀번호로 설정된 비밀번호가 유출될 경우에는 허가되지 않은 사용자가 접근할 수 있는 상황이 생길 수 있지만, 한번 사용된 비밀번호는 초기화가 되므로 비밀번호가 유출되더라도 허가되지 않은 사용자가 접근하는 가능성은 매우 희박하다.

2.4 RF 통신과 블루투스 통신

RF 통신은 무선통신에 사용되는 주파수로서 현재 자동차 스마트키 등에 자주 사용되고 있으며, 특정한 주파수를 감지하여 송신된 주파수를 검사한 주파수와 일치할 경우에 통신을 허용하게 된다. 자동차 스마트키에서는 RF 통신이 이모빌라이저와 같이 사용되어 설정된 IoT 기기의 사용자와 일치하는지를 확인하는 인증의 용도로 사용되고 있다.

블루투스는 RF 통신과 같은 무선 통신 방식 중 하나로 디바이스간 동기화를 통해 통신을 하게 된다. 블루투스 통신 방식은 보안성과 호환성, 저전력 등의 이유로 IoT 기기에 자주 사용이 되고 있으며, 특히 스마트폰에 활용이 많이 되고 있다.

<표 3> 블루투스 버전에 따른 특징

	블루투스 1.x	블루투스 2.x	블루투스 3.x	블루투스 4.x
개발시기	1998	2004	2009	2010
전송 속도	500Kbps	1~3Mbps	1~3Mbps(최대 24Mbps)	1Mbps
전력소모	많다	적다	많다	매우적다
보안	낮다 ----------> 높다			
제품	핸드폰,핸즈프리	헤드셋,마우스	PMP,UMPC	건강,가전,비콘,임베디드 등등

<표 3>과 같이 블루투스 버전마다 각 특징이 있으며 현재는 2016 년에 공개된 블루투스 5 버전까지 개발된 상태이다 [9].

3. 보안 설계 및 구현

본 장에서는 디지털 도어락의 보안 기능을 강화하기 위한 설계 기법과 구현 결과를 설명한다. 디지털 도어락을 구현하기 위하여 프로토타입으로 아두이노와 라즈베리 파이 등의 하드웨어를 사용하고 있다.

3.1 보안 설계

보안 설계를 위하여 기존 디지털 도어락에 존재하는 보안 기능에 대한 편리성을 강화하고 디지털 도어락에 대한 접근을 제한할 수 있는 인증 기능과 취약성 보완을 중심으로 설계하였다.

<표 4> 보안 기능 설계

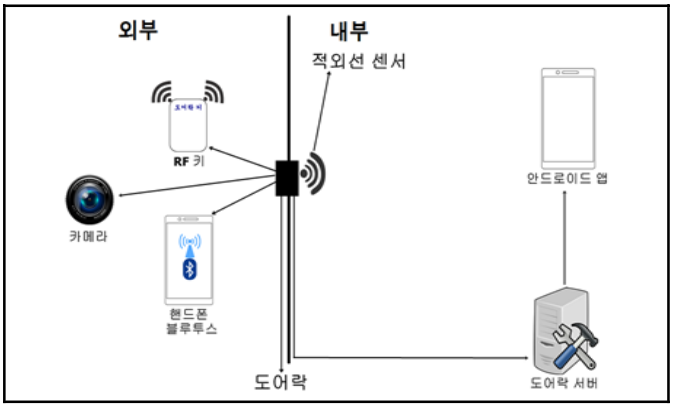
구분	기능	설명
H/W	적외선 센서	적외선 센서를 통한 내부 기능 제어
	이중 잠금	내부에서 잠금을 활성화하여 외부 침입 방지
	비밀번호 OTP	OTP기능을 사용하여 비밀번

		호 보안 강화
	RF 통신 스마트키	RF 통신을 사용하여 인증 요소 추가를 통한 보안 강화
	블루투스 페어링	무선 통신 방식을 이용한 다른 기기와의 연계
	얼굴 인식 카메라	디지털 도어락에 카메라를 장착하여 외부 확인 및 얼굴 인식 기능을 도입
S/W	디지털 도어락 모바일 앱	스마트폰과 아두이노 사이에 블루투스 페어링 기능을 활용한 모바일 연동
	얼굴 인식 기능	사용자 얼굴 사진을 캡처하여 DB 에 저장한 뒤 출입을 시도하려는 사용자의 얼굴과 대조

<표 4>는 기존 디지털 도어락에서 제공하는 기능과 이러한 보안 기능을 보완할 수 있는 설계 기준을 보여주고 있다.

3.2 보안 구현

보안 구현은 디지털 도어락을 기준으로 내부와 외부로 구분하여 구현하였으며, 디지털 도어락 본체의 경우 라즈베리 파이 3 B+ 모델과 아두이노 Mega 2560 모델을 사용하여 기능을 구현하였다.

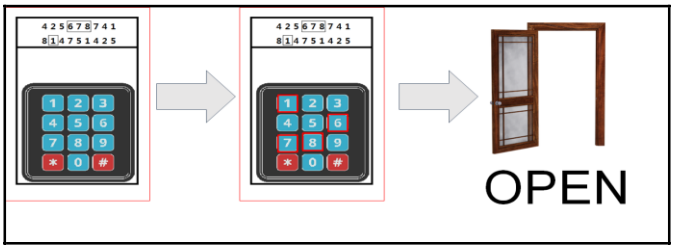


(그림 3) 보안 구현 구분도

3.3 외부 보안 기능

외부 보안은 비밀번호 OTP, RF 무선통신을 이용한 스마트키, 얼굴인식 카메라, 블루투스 무선통신을 이용한 모바일 앱과의 연동기능을 추가하였다. 외부 보안 기능들은 현재 디지털 도어락에서 자주 사용되는 모델들이 가지고 있는 허수 기능 보안이 사용하기 번거롭다는 단점과 패스워드에 대한 편리성을 강화하였고, 허가되지 않은 사용자의 접근을 이차적인 인증을 통하여 방지하고자 하였다.

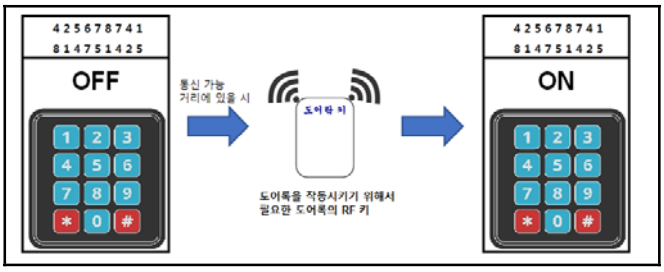
비밀번호 OTP 의 경우에는 스크린에 매번 랜덤한 숫자가 생성되며, 기존의 비밀번호를 외우는 방식이 아닌 위치를 기억하여 입력하는 방식으로 구현하였으며 도중에 잘못 입력하였을 경우에는 번호 재생성 기능과 5 회 이상 실패하면 5 분간 잠금 기능이 작동하도록 구현하였다.



(그림 4) 비밀번호 OTP

기존 디지털 도어락의 취약점으로 지문 채취, 카메라 녹화를 통한 비밀번호 탈취를 방지하는 기능 등에 사용된 허수 기능을 OTP 기능을 도입하였고, 지문이 설정된 비밀번호에만 남지 않고 골고루 분포되도록 유도하였다. 그리고 다른 취약성인 쉬운 비밀번호 설정 같은 문제도 다른 비밀번호로 초기화되는 특징을 이용하여 매번 비밀번호가 변경되는 효과를 얻도록 하고 있다.

RF 무선통신의 경우에는 자동차 스마트키에서 사용하는 방법을 고려하였다.



(그림 5) RF 무선통신 스마트키

(그림 5)와 같이 휴대용 디지털 도어락 키가 특정 주파수를 뿌리게 되고 디지털 도어락에서 이를 감지하여 같은 주파수일 경우에만 비밀번호 입력 기능이 활성화되도록 하였다. 이를 통하여 외부 인증 절차를 추가할 수 있으며, 허가된 사용자만 다음 인증 절차를 수행할 수 있도록 설계하였다. 이러한 보안 기능으로 공격자가 비밀번호를 알게 되더라도 이차적인 보안을 통하여 접근이 불가능하도록 하였다.

또한, 생체 인식 보안 기능 중 하나인 얼굴 인식 기능을 디지털 도어락에 적용하였다. 도어락 외부에 카메라를 설치하고 데이터베이스에 사용자 얼굴을 저장하여 비교하는 방식을 사용한다.

(그림 6) 카메라를 통한 얼굴 인식 시스템

외부 카메라를 통해 인증 시도를 하는 사용자의 얼굴이 찍히게 되고, 서버의 데이터베이스에 등록되어 있는 얼굴 표본들과 비교하고 등록이 되어있는 사용자인지 확인 절차를 거친다. 이러한 과정을 통하여 일치하는 경우에만 문을 열어주는 방식으로 보안 기능이 수행된다.

다음으로 블루투스 무선통신 기능을 이용해 스마트폰과 같은 외부요소와 연동하는 것으로 블루투스 페어링 기능을 이용하여 스마트폰 앱과의 연동을 통해 도어락 출입 로그와 얼굴 인식 카메라 등과 연계함으로써 현재 집 내부에 있는 구성원을 확인할 수 있도록 제공하여 보안을 강화한다.

3.4 내부 보안 기능

내부 보안으로는 적외선 센서를 이용한 내부 기능 제어를 구현하였다. 내부 보안 기능들은 기존 디지털 도어락에서 많이 구현되어 있는 이중 잠금 기능을 자동적으로 작동하게 하여 편리성을 강화시키고 외부에서 물리적인 힘으로 내부의 기능을 강제적으로 작동시키는 것을 적외선 센서를 이용하여 내부 이용자 유무 인식을 통한 인증으로 설계하였다. 또한, 적외선 센서의 물체 인식 기능을 이용하여 내부 기능들을 제어할 수 있도록 하고 있다.

(그림 7) 적외선 센서를 이용한 내부 기능 제어

(그림 7)과 같이 내부에 존재하는 버튼을 누르면 문이 열리는 기능을 제어하고 이중 잠금 기능의 편리성을 강화시킬 수 있도록 하고 있다. 내부 잠금 해제 버튼의 경우에는 외부에서 물리적인 힘으로 강제적으로 내부 기능 접근을 통해 열림 버튼을 사용하는 사례가 발생하지 않도록 적외선 센서 인식 기능을 이용하여 내부에 사람이 접근하는 것을 확인하여 내부 사용자가 인식이 되었을 경우에만 열림 버튼을 활성화시키는 방식으로 보완하였다.

4. 결론 및 향후 연구 방향

본 논문에서는 디지털 도어락 사용의 증가로 발생하는 보안 취약점을 분석하고, 보안 기능이 강화된 디지털 도어락을 설계하고 구현하였다. 또한, 현재 제공되는 보안 기능이 편리성 부족으로 사용되지 않는 문제를 보완할 수 있는 기능을 추가적으로 제공한다. 제안된 시스템에서는 디지털 도어락을 중심으로 내부와 외부 기능으로 구분하고, 각각에서 별도로 제공되는 보안 강화 기능을 제공함으로써 지능화된 해킹 공격 및 개인 정보 유출을 방지할 수 있도록 설계하고 구현하였다.

향후 계획은 차별화된 새로운 보안 기능을 제시하여 새로운 해킹공격에 강인한 시스템 구현에 반영하고자 한다.

감사의 글

본 논문은 과학기술정보통신부 정보통신창의인재양성사업의 지원을 통해 수행한 ICT 멘토링 프로젝트 결과물입니다.

참고문헌

[1] 디지털 도어락 국내시장 집중분석, 2019. https://www.boannews.com/media/view.asp?idx=79876
[2] 미국시장의 문, 디지털 도어록, 2017. https://www.boannews.com/media/view.asp?idx=54619&page=1&kind=3
[3] 혜강씨큐리티 디지털 도어락 보안 기술, http://www.h-gang.co.kr/technology/index.asp?pIdx=t_2
[4] Gateman 디지털 도어락 보안 기술, https://www.egateman.co.kr/ko/technology/
[5] Samsung SDS 디지털 도어락 보안 기술, https://www.samsungsds.com/global/ko/solutions/off/cddl/smart_doorlock.html
[6] 구멍 뚫린 스마트홈, 2019 https://www.mk.co.kr/news/business/view/2019/07/547509/
[7] Arduino, https://www.arduino.cc/
[8] Raspberry Pi, https://www.raspberrypi.org/
[9] Wikipedia, https://ko.wikipedia.org/wiki/
[10] 이가연, 박용범, 이동수, 김진술, “라즈베리파이를 이용한 IoT 기반 스마트 도어락 개발”, 한국정보기술학회 종합학술발표논문집, pp. 597-600, 2019.
[11] 김윤수, 김정태, “RFID 모듈을 이용한 디지털 도어락의 설계”, 한국정보통신학회 학술대회논문집, pp. 59-60, 2013.
[12] 박일도, 김덕수, 김종오, “스마트 폰을 이용한 블루투스 도어락 시스템 구현”, 대한전자공학회 학술대회, pp. 1461-1464, 2017.