JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 21, No. 5 : 1027~1034 May. 2017

시간 동기 방식의 OTP를 이용한 디지털 도어락 시스템

황형진 · 김권양 · 하일규*

A Digital Door Lock System Using Time- Synchronous One Time Password

Hyung-Jin Hwang · Kweon-Yang Kim · Il-Kyu Ha*

Department of Computer Engineering, Kyungil University, Gyeongsan 38428, Korea

요 약

최근 들어 개인 정보 유출을 방지하고, 보안을 강화하기 위하여 OTP (One-time- Password)를 이용한 로그인 방법을 많이 사용하고 있다. OTP 방식은 은행의 개인 계정 보안을 위하여 주로 사용되어온 방법으로 일회용 비밀번호를 받아 사용하는 보안성이 강화된 방법 중 하나이다. 한편, 일상생활에서 자주 사용하는 디지털 도어락은 편의성과 보안성을 동시에 요구한다. 디지털 도어락에 관한 관련 기술이 발전하고 있지만 아직 보안성에는 취약한 것이 사실이다. 특히, 가장 흔하게 사용되고 있는 비밀번호 입력 방식의 디지털 도어락은 편의성을 제공하지만 비밀 번호 노출, 망각 등과 같은 부작용이 따르게 된다. 따라서 본 연구에서는 비밀 번호 노출과 망각의 위험이 없는 보안성과 편의성이 강화된 OTP 기반의 디지털 도어락 시스템을 제안하고 구현한다.

ABSTRACT

Recently, OTP (One-time-Password) log-in methods have been used in many areas to prevent leakage of personal information and enhance security. The OTP method is primarily used for security of bank personal account, this is one of the sophisticated security ways in which one time password is generated and checked to enhance security. Digital door locks frequently used in everyday life require convenience and safety simultaneously. Meanwhile, related technologies for digital door locks are evolving, but methods for enhancement of security are still unsatisfactory. Generally, the digital door lock using password input type has been most commonly used and especially it provides more convenience, but it has some problems such as password exposure and password oblivion. Therefore, in this study, we propose and implement the OTP-based digital door lock system with enhanced security and convenience features but without the risk of password exposure and oblivion.

키워드 : One Time Password, 디지털 도어락, 디지털 도어락 암호화, OTP 응용

Key word : About One Time Password, Digital Door Lock, Digital Doorlock Encryption, OTP Application

Received 10 January 2017, **Revised** 01 February 2017, **Accepted** 14 February 2017

* **Corresponding Author** Il-Kyu Ha(E-mail:ikha@kiu.kr, Tel:+82-53-600-5564)
Department of Computer Engineering, Kyungil University, Gyeongsan 38428, Korea

Open Access https://doi.org/10.6109/jkiice.2017.21.5.1027 print ISSN: 2234-4772 online ISSN: 2288-4165

ⓒThis is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(http://creativecommons.org/li-censes/ by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright Ⓒ The Korea Institute of Information and Communication Engineering.

Ⅰ. 서 론

최근 들어 개인 정보에 대한 중요성이 강조되고 있지만 여러 분야에서 개인 정보가 유출되는 사례가 일어나고 있다. 이러한 개인 정보 유출을 방지하고, 보안을 강화하기 위하여 최근에는 OTP (One-time- Password) 방법[1]을 이용한 로그인 방법을 사용하고 있다. OTP 방식은 은행의 개인 계정 보안을 위하여 주로 사용되어온 방법으로 일회용 비밀번호를 받아 사용하는 보안성이 강화된 방법이다. 최근에는 스마트폰의 대중화로 OPT 로그인 방식이 다양한 어플리케이션에 적용되고 있다.

한편 생활의 필수 제품으로 자리 잡고 있는 디지털 도어락은 사용이 증가하고 있지만 한편으로 여러 가지 부작용을 일으키기도 한다. 즉, 키 없이도 사용할 수 있는 편리함을 주기도 하지만 비밀번호의 노출, 비밀번호의 망각 등 다양한 부작용 사례를 일으킨다.

본 논문에서는 이러한 일상생활에서 자주 이용하는 디지털 도어락의 보안성과 편의성을 강화하는 방안으로 디지털 도어락에 OTP 방식을 적용하는 방법을 연구한다. OTP 방식을 적용함으로써 비밀번호 노출의 위험을 줄일 수 있고, 비밀번호 망각의 부담을 감소시킬 수 있으며, 허가받지 않은 출입자의 무단침입을 막으며, 네트워크를 통하여 언제 어디서든지 출입기록을 확인할 수 있는 다양한 기능을 가진 OTP기반 디지털 도어락 시스템을 제안하고 구현한다.

Ⅱ. 관련 연구

2.1. OTP 방식

One Time Password(OTP)는 일회용 패스워드로 거래와 조회 등을 위한 개인의 인증 수단 중 하나이다. OTP는 은행 업무, 게임 등 다양한 분야에서 보안성을 강화하기 위한 방법으로 사용되고 있다. OTP 방식은 질의응답(Challenge-Response) 방식, 시간 동기(Time-Synchronous) 방식, 이벤트 동기화(Event-Synchronous) 방식, 조합 방식 등으로 나뉜다[2,3]. 질의 응답 방식은 사용자와 패스워드 생성 서버가 상호작용하면서 사용자가 알고리즘에 따라 값을 주고받으면서 사용자를 인증하는 방식이다. 시간동기화 방식은 질의 응답 방식의 패스워드 생성 절차의 번거로움을 개선한 방식으로서 시간 정보를 OTP 생성 입력 값으로 사용하는 방식이다[4]. 이벤트 동기화 방식은 서버와 사용자 단말기가 시간 정보 대신 동일한 카운트 값을 기준으로 비밀번호를 생성하는 방식이다. 조합 방식은 시간 동기화 방식과 이벤트 동기화 방식을 조합한 방식이다. 즉, OTP 생성을 위한 값으로 시간 정보와 카운트 값을 모두 이용하는 방식이다[5,6].

2.2. 디지털 도어락의 보안 방법

현재까지 디지털 도어락의 보안성과 편의성 강화를 위해 다양한 연구들이 진행되어 왔다. 지금까지 디지털 도어락의 보안 방식은 비밀번호 입력 방식, 카드인식 방식, 반도체칩 방식, 지문 및 생체 인식 방식 등으로 발전되어 왔다. 또한 최근 들어 IoT 기술의 발전과 함께 다양한 통신방식을 통한 원격제어 방식이 연구되고 있다. 디지털 도어락의 보안성 및 편의성 강화에 관한 대표적인 연구는 표 1과 같은 것이 있다. [7]은 편의성을 향상하기 위하여 원격제어 기능, 정당한 사용자의 접근 시 자동 열림 등의 기능을 갖추고 있으며, 보안성을 향상하기 위하여 비밀번호의 주기적 변경 기능, 일정 횟수 이상 비밀번호 입력 오류 시 접근자 촬영 및 전송 등의 기능을 갖추고 있다. [8]은 PGA(Principal Component Analysis) 패턴인식 기법을 이용하여 출입자의 영상을 촬영하여 서버로 전송하고 데이터베이스의 정보와 일치여부를 판정하여 도어락을 원격 개방하는 방식이다. [9]는 접근하는 객체와 움직임을 인식하고 일정 근접범위에 있는 객체의 영상을 촬영하여 사용자의 모바일 장치와 관리 서버로 전송하는 기능을 갖추고 있다. 다만 서버의 자동 인식에 의한 자동 개방 기능은 갖추고 있지 않다. [10]은 사용자가 출입하고자 하는 도어락의 MAC address를 Bluetooth로 읽고 이를 스마트폰의 앱에 저장된 미리 허가된 MAC address 정보와 일치여부를 확인하여 도어락을 개방하는 방식이다. 또한 앱을 통하여 정당한 사용자의 등록을 통해 키를 공유할 수 있는 기능을 갖추고 있다. [11]은 실외에서 스마트폰으로 실내의 도어락 컨트롤러를 원격제어하는 응용으로서 Bluetooth 통신을 이용한다. [12]는 보안성을 강화하는 방법으로 도어락 기기를 실내로 숨기고 증강현실을 이용하여 도어락을 사용자의 스마트폰 화면에 띄우는 방법을 사용한다. 또한 메모 기능을 갖추어 사용자 간의 의사소통을 원활하게 하는 기능을 갖추고 있다.

[13]은 비밀번호 입력대신 노크의 패턴을 패스워드로 사용하는 방법을 연구하고 있다. [14]는 비밀번호 입력의 번거로움을 덜기 위하여 음성 인식을 이용하여 도어락을 개방하는 방법을 제시하고 있다. 디지털 도어락이 건물 외부에 노출되어 있을 경우 눈과 비 등 날씨 변화에 취약하다. 따라서 [15]는 디지털 도어락을 유리문 뒤의 실내에 두고 자기장을 이용하여 도어락을 개폐하는 방법을 제안하고 있다. [16]은 보안성을 강화하기 위한 방법으로 출입자의 동영상 스트림을 사용자에게 전송하고 사용자가 신원을 확인 한 후 원격으로 개방하는 방식을 연구하고 있다. [17]은 RFID 태그를 이용하여 근거리에 있는 태그 정보를 인식하고 도어락 컨트롤러를 통해 도어락을 개방하는 방식이다.

Table. 1 Comparison of security methods of digital door lock

Paper	Security Type	Features	Technology
[7]	Password	Periodic Password Change Invader Image Transmission	Bluetooth
[8] [9]	Face Recognition	Face Recognition	PCA
[10]	MAC address Recognition	hand-free opening Key sharing	Bluetooth GCM
[12]	Password	Augmented Reality	WiFi AR
[13]	Analog Signal (vibration)	Vibration Recognition (Knock Rhythm Recognition)	Vibration Sensor
[14]	Voice Recognition	Voice Recognition	Voice Sensor
[15]	Password	Magnetic Field Recognition	Magnetic Recognition
[16]	Password	Video Stream Transmission	
[17]	RFID tag	RFID	RFID
This paper	Time Synchronous OTP	Using pre-registration Seed value and time	OTP

이와 같이 디지털 도어락은 다양한 편의기능과 보안기능이 있지만 보안위협이 존재한다. 비밀번호 입력방식은 키패드를 통해 입력하게 되므로 비밀번호의 노출 위협이 있다. 카드방식과 반도체칩 방식은 카드 키 분실 시 복제의 위협이 있다. 지문 및 생체인식 방식 또한 지문의 복제 가능성이 있다. 이러한 문제들은 대부분 비밀번호가 정적(static)으로 유지되기 때문이다. 이러한 문제를 해결하기 위해 본 연구에서는 OTP를 이용하여 동적(dynamic)으로 비밀번호를 바꿔 비밀번호의 노출을 막는 시간 동기화 방식OTP를 이용한 디지털 도어락 시스템을 제안하고 구현한다.

Ⅲ. OTP기반 디지털도어락 시스템 설계

3.1. 디지털 도어락 시스템 OTP 생성 및 인증 과정

제안한 시스템은 시간동기화 OTP방식을 디지털 도어락에 적용시킨 것으로서 그림 1과 같은 비밀번호 생성 및 인증 과정을 거친다. 디지털 도어락과 사용자의 스마트폰에서 각각 동일한 OTP생성 알고리즘을 작동시키고, 시간과 시드값을 가지고 OTP를 생성한다. 사용자는 스마트폰에서 최대 8자리로 구성되는 시드값을 입력하여 OTP를 생성하고 이를 디지털 도어락에 입력하고 도어락 컨트롤러는 자체에서 생성된 OTP와 비교하여 일치여부를 판단함으로써 정당한 사용자임을 인증한다.

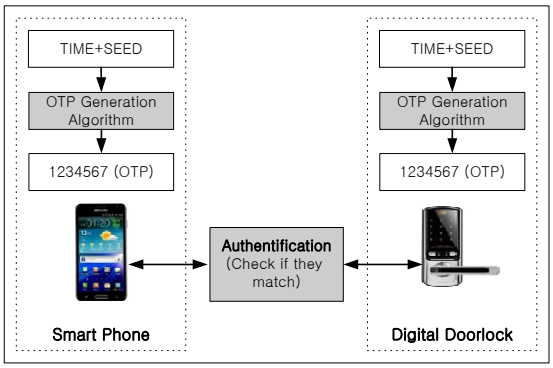

Fig. 1 Certification Process of time-synchronous OTP method

3.2. 제안한 OTP기반 디지털 도어락 시스템의 주요기능

제안한 시스템은 다음과 같은 기능을 가지도록 설계한다. 첫째, 비밀번호의 노출을 최소화하여 보안성을 높이기 위해 OTP기반 비밀번호 인증이 이루어지도록 한다. 둘째, 보안성을 보다 강화하기 위하여 연속적

으로 비밀번호 입력 오류 시 출입자의 동영상을 촬영하여 사용자(집소유자)에게로 전송하도록 한다. 셋째, 사용자의 편의성을 향상하기 위하여 출입에 대한 로그 정보를 유지하고 사용자의 스마트폰으로 전송하도록 한다. 넷째, 편의성을 증진하기 위한 다른 방법으로서 사용자의 스마트폰에서 원격개폐가 이루어질 수 있도록 한다. 이때 사용자의 단말기에서 생성한 OTP 코드를 라즈베리파이로 전송하여 인증하도록 하는 방식을 택한다.

3.3. OTP 기반 디지털 도어락 시스템의 보안 동작

제안한 OTP 기반 디지털 도어락 시스템의 보안을 위한 동작과정은 그림 2와 같다. 사용자가 비밀번호를 입력할 때 도어락은 입력을 받은 비밀번호와 생성된 비밀번호를 비교한다. 만약 일치한다면 도어락은 개방되며, 3회 실패 시 라즈베리파이 컨트롤러에 부착되어 있는 카메라를 통하여 특정시간 동안 출입자의 동영상을 촬영한다. 촬영된 동영상은 라즈베리파이 컨트롤러의 SD 카드에 1차로 저장이 되며, 추후 인터넷 등 외부망을 통하여 사용자에게 팝업 메시지로 알린다. 또한, 출입 로그가 저장되고 스마트폰에 전송되어 원격의 사용자가 출입 정보를 확인할 수 있다. 사용자는 촬영된 동영상을 확인한 후 정당한 사용자 여부에 따라 원격 개방을 하거나 경비업체 또는 주변 경찰서에 신고할 수 있다. 사용자의 스마트폰으로 전송된 동영상은 스마트폰의 메모리를 많이 차지 할 수 있으므로 일정 용량 이상의 메모리가 쌓였을 때 동영상의 삭제 알람을 주어 빈 공간을 확보를 할 수 있다.

제안된 시스템은 다음과 같은 장점을 가진다. 첫째, 동적 비밀번호의 사용으로 비밀번호 노출의 위험이 없다. 비밀번호가 노출되었다 하더라도 OTP 비밀번호는 일회용으로 사용되기 때문에 추후에는 사용할 수 없다. 둘째, 비밀번호 기억의 부담감이 없다. 비밀번호는 출입할 때마다 새롭게 생성되는 OTP 비밀번호를 사용하므로 사용자는 비밀번호를 사전에 기억할 필요가 없다. 셋째, 부가적인 기능으로 편의성을 증진할 수 있다. 즉, 출입자의 로그 정보, 무단 출입자의 동영상 정보 등이 사용자에게 전송되어 사후 조치를 할 수 있게 하고, 정당 출입자임을 확인하고 원격으로 개폐할 수 있는 기능을 제공한다.

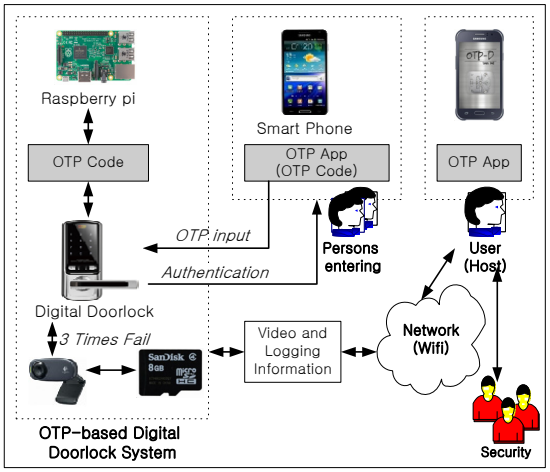

Fig. 2 Security operation of the OTP-based digital door lock system

Ⅳ. OTP기반 디지털 도어락 시스템 구현

4.1. 디지털 도어락 컨트롤러의 동작

그림 3은 제안된 디지털 도어락 시스템의 비밀번호 인증을 위한 알고리즘을 보여준다. 사전준비 단계로서 사용자는 미리 알고리즘에 OTP 생성을 위한 최대 8자리 정수의 seed 값을 설정해준다. 이후 사용자의 스마트폰과 디지털 도어락은 위성시간 정보획득 API를 이용하여 현재의 시간정보를 얻고 서로 시간 동기화를 한다. 다음은 OTP 코드 생성단계이다. 디지털 도어락은 seed값과 시간값을 읽고, 이로부터 OTP 코드를 생성한다. 생성한 코드는 OTP 인증프로그램, 즉 APO (Authentication Program for OTP)에 인증을 위한 값으로 설정한다. 마지막 단계는 OTP 코드를 이용한 출입자 인증단계이다. 우선 코드입력오류 횟수를 카운트하기 위한 변수 CNT를 0으로 초기화한다. 사용자의 OTP 입력이 계속 되는 동안 출입자로부터 OTP 코드(비밀번호)를 입력받고 이를 APO에 설정된 코드와 비교한다. 만약 일치한다면 도어락은 오픈되며, 그렇지 않은 경우 코드입력오류 횟수를 1증가 시킨다. 만약 코드입력오류 횟수가 3회에 도달하면 카메라 작동을 위한 함수가 실행되어 출입자의 영상이 촬영된다. 이후 CNT는 다시 0으로 설정되고 출입자로부터 다음 OTP 코드를 입력받는다.

```
//Control Algorithm for the OTP-based Doorlock
//Preperation Stage
1. set seed value  // set a seed value to the algorithm
2. time synchronization // between phone and doorlock
//OTP creation Stage
3. read seed value and time value
4. generate OTP code
5. set of OTP authentication value -> APO
//OTP authentication Stage
6. set 0 to CNT //CNT is a variable for error counting.
7. while not end of OTP input
8.     read password from person entering
         K= {x1,x2,...,xn}
9.   if K ≠ OTP code of APO
10.    CNT = CNT +1
11.    if CNT == 3
12.        call cemera.sh(camera function)
13.        set 0 to CNT
14.      end if
15.    else
16.        open door
17.    end if
18.    read next OTP input
19. end while
```

Fig. 3 Control algorithm for the proposed digital door lock control

4.2. 제안 시스템의 구현을 위한 HW 및 SW 구성

제안된 OTP 기반 디지털 도어락 시스템의 구현을 위한 하드웨어 및 소프트웨어 구성요소는 표 2와 같다. 도어락 컨트롤러로는 Raspberry Pi3가 사용되고, 운영체제로는 Rasbian을 사용하며, 모바일 앱을 위한 웹서비스로 UHTTPD가 사용된다. 서버에 저장된 데이터에 접근하기 위해 MySQL과 리눅스 Shell 프로그래밍을 위해 Python이 사용된다. 출입자로부터 OTP 코드(비밀번호)를 입력받기 위해 4x4 멤브레인 키패드를 사용한다. 출입자가 OTP 생성 모바일 장치를 소지하고 디지털 도어락에 접근하였을 때 디지털 도어락이 모바일 장치의 OTP 코드를 자동으로 인식하고 비교하기 위하여 블루투스 장치를 필요로 한다. 원격지의 사용자(주인)와 디지털 도어락은 Wifi 신호를 이용하여 통신한다.

Table. 2 Hardware components for implementation of the proposed system

Component	Specifications	Function
Microcontroller	Raspberry Pi3	Controller
Operating System	Rasbian Jessie	Operating System
Web Server	UHTTPD	Mobile App. Service
Database	MySQL	Data Storage
Language	Python, Java	DB access, Shell, App
Card Reader	Real Time	Surveillance
Mobile Device	Galaxy note 5	Mobile Device
Digital Doorlock	Miller	Main Device
Input Pad	4x4 Matrix Key Pad	Input Module
Communication Module	HC-03	Bluetooth Module

4.3. 사용자를 위한 모바일 앱

OTP기반 디지털 도어락을 사용하는 출입자와 사용자(주인)의 편의성을 높이기 위한 모바일 앱이 필요하다. 출입자는 로그인을 통하여 모바일 앱에 접근할 수 있고 OTP 생성기능을 통하여 OTP 코드를 생성할 수 있다. 제안하는 디지털 도어락 시스템은 시간 동기화 방식을 이용하기 때문에 출입자의 스마트 폰과 디지털 도어락은 같은 시간 값을 가져야 동일한 OTP를 생성한다. 시간 값은 도어락을 처음 작동 시킬 때 한번 위성시간정보 API를 통하여 현재의 시간 정보로 동기화한다. 이후에는 디지털 도어락과 출입자의 모바일 장치 간의 동일한 알고리즘을 통해 OTP를 생성할 수 있다. 사용자(주인)의 편의성 증진을 위하여 디지털 도어락의 출입정보를 조회할 수 있는 기능이 있다. 디지털 도어락이 작동한 정보를 통해 사용자의 출입 정보를 확인할 수 있다. 또한 잘못된 OTP 코드(비밀번호)를 3회 이상 입력하였을 경우 출입자의 영상이 촬영되고 촬영된 출입자의 영상을 확인할 수 있는 기능이 있다. 만약 정당한 출입자가 아닌 경우, 보안업체 또는 관계기관에 신고할 수 있다. OTP생성을 다시 시행할 수 있도록 하기 위한 Reset 기능을 갖추고 있다. 그림 4는 출입자와 사용자(주인)을 위한 앱의 구성을 보여준다. 그림 5는 구현된 모바일 앱의 주요 화면들을 보여준다.

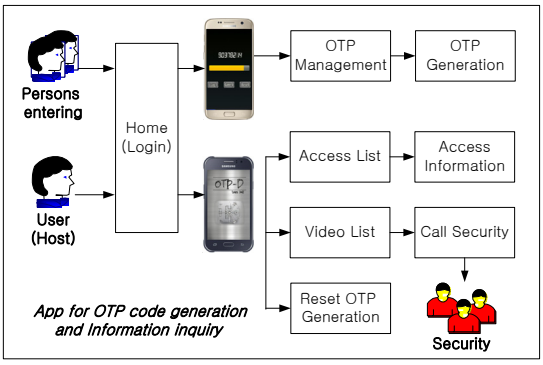

Fig. 4 App Configuration for users

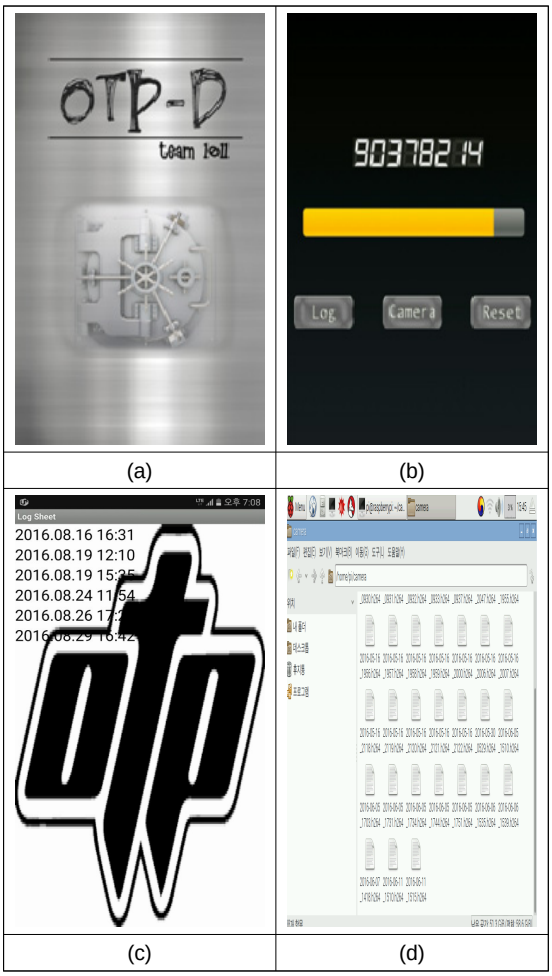

Fig. 5 Main screens of the implemented apps (a. Main screen b.OTP creation c.User access log d.Shooted videos)

그림 5의 (a)는 OTP기반 도어락 시스템을 위한 앱의 메인 화면이다. 출입자와 사용자(주인)은 로그인을 통하여 사용 메뉴로 진입할 수 있다. (b)는 OTP 생성화면이다. 화면의 상단에 생성된 OTP코드가 보여지고 코드의 유효 시간이 아래에 노란색 막대로 표시된다. 유효시간은 1분으로 설정되어 있고, 1분이 지나면 새로운 OTP코드가 생성된다. 출입자는 생성된 코드를 디지털 도어락에 입력하여 출입 인증을 받는다. (c)는 디지털 도어락이 작동한 정보를 보여준다. 사용자는 이를 통하여 출입 기록을 확인할 수 있다. (d)는 출입자가 3회 이상 비밀번호 입력 오류 시 촬영된 영상의 리스트를 보여준다.

4.4. 구현된 OTP기반 디지털 도어락 시스템

그림 6은 구현된 디지털 도어락 시스템을 보여준다. 디지털 도어락은 인바디와 아웃바디로 구성되어 있다. 인바디에는 장금장치 기능을 갖춘 도어락 장치가 있으며, 아웃바디는 키패드, 카메라 모듈, 마이크로 컨트로러 등으로 구성된다. 구현상의 가장 큰 문제 중 하나는 디지털 도어락 장금장치의 전력공급문제이다. 라즈베리파이는 마이크로 컨트롤러는 3.3V 출력을 사용하지만, 도어락의 장금장치 모터는 3.3V로 작동되지 않고 계폐 도중 멈추는 현상이 발생한다. 이에 대한 해결 방법으로 본 연구에서는 릴레이보드를 사용한다. 그림과 같이 라즈베리파이의 브레드보드 회로 위쪽에 릴레이보드가 부착되어 있다.

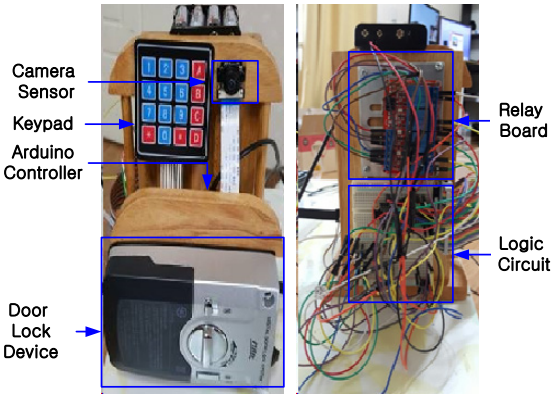

Fig. 6 The implemented OTP-based digital door lock system

릴레이 보드는 라즈베리파이에서 GPIO 신호를 받은 뒤 건전지 4개를 병렬 연결하여 외부 출력을 준다. 따라서 도어락 장금장치 모터에 5v의 출력을 주어 정상적인 계폐가 가능하게 한다. 멤브레인 키보드를 이용하여 OTP 패스워드 입력이 가능 하며, 멤브레인 키보드 옆에 위치한 RPi카메라를 이용하여 악의적인 침입자가 비밀번호 3회 입력 실패 시 촬영을 하도록 구현된다.

Ⅴ. 결 론

디지털 도어락의 보안성과 편의성을 강화하기 위한 다양한 연구들이 진행되어 왔지만 비밀번호 노출 또는 망각의 문제는 해결하기 어려운 문제이다. 본 논문에서는 동적인 비밀번호를 가지는 시간 동기 방식의 OTP를 이용한 디지털 도어락의 시스템을 설계하고 구현하였다. 동적인 비밀번호를 가지므로 기존 비밀번호가 노출되더라도 안전성을 높일 수 있다. 또한 비밀번호 망각의 문제점을 해결할 수 있다.

즉시 생성된 OTP 코드를 비밀번호로 이용하므로 망각의 문제는 발생하지 않는다. 본 연구는 금융권 등에서 이용되어 오던 OTP 코드 인증 방식을 디지털 도어락에 적용한 사례이다. 기존 도어락이 가지고 있던 비밀번호 노출 또는 망각의 문제를 해결하여 보안성을 강화하였다. 바쁘게 살아가는 현대인이 일상생활에서 편리하게 사용할 수 있는 도어락 방식이지만, 비밀번호 입력을 위하여 스마트 장치가 필요하고 앱을 실행하여 비밀번호를 생성하여야 하므로 자주 출입하는 출입문에서는 불편할 수 있다. 향후 스마트 장치에서 생성된 비밀번호를 근거리 통신으로 디지털 도어락에 전달하고 인증과정을 거쳐 도어락을 개폐하는 추가적인 연구를 시행할 계획이다.

REFERENCES

[1] Internet Std. Network Working Group RFC 2289, “A One-Time Password System,” IETF, Fremont, CA, 1998.

[2] D. Choi, W. Kim and D. Won, “One-Time Password Technology Analysis and Standardization Trend,” *Review of KIISC*, vol. 17,no. 3, pp. 12-17, Jun. 2007.

[3] S. Seo and W. Kang, “OTP Technology Status and OTP Introduction Example,” *Review of KIISC*, vol. 17, no. 3, pp. 18-25, Jun. 2007.

[4] Internet Std. Network Working Group RFC 6238, “*TOTP: Time-based one-time password algorithm*,” IETF, Fremont, CA, 2011.

[5] Y. Kim, J. Han, Y. Jeon and J. Kim, “Implementation of a MTM-based secure OTP Generator for IoT Devices,” *Journal of embedded systems and applications*, vol. 10, no. 4, pp. 199-206, Aug. 2015.

[6] S. Song and K. Kim, “OTP Strandardization trends at home and abroad,” *Review of KIISC*, vol. 22, no. 2, pp. 30-36, Apr. 2012.

[7] I. Ha, “Security and Usability Improvement on a Digital Door Lock System based on Internet of Things,” *International Journal of Security and Its Applications*, vol. 9, no. 8, pp. 45-54, Sep. 2015.

[8] J. Lim, C. Kim, W. Cha, T. Han, G. Huh, S. Song and S. Lee, “Reliable Digital Door Lock Control System using Face Recognition,” *Journal of IKEEE*, vol. 17, no. 4, pp. 499-504, Dec. 2013.

[9] S. Lee, J. Park, B. Woo and H. Choi, “Video Digital Doorlock System for Recognition and Transmission of approaching Objects,” *KIPS Transaction: Software and Data Engineering*, vol. 3, no. 6, pp. 237-242, Jun. 2014.

[10] D. Seo, H. Ko and Y. Noh, “Design and Implementation of Digital Door Lock by IoT,” *KIISE Transactions on Computing Practices (KTCP)*, vol. 21, no. 3, pp. 215-222, Mar. 2015.

[11] J. Potts and S. Sukittanon, “Exploiting Bluetooth on Android Mobile Devices for Home Security application,” in *Proceedings of IEEE Southeastcon*, Orlando: FL, pp. 1-4, 2012.

[12] K. Lee and J. Kim, “Design and Implementation of Hybrid VR lock system by Arduino Control,” *Journal of the institute of signal processing and systems*, vol. 15, no. 3, pp. 97-103, Jul. 2014.

[13] M. Choi, D. Cho, S. Kim and T. Jin, “Digital Door-Lock System Controlled with Analog Signal,” in *Proceedings of 2013 ICROS/KROS/KIIS*, Busan, vol. 2013, pp. 55-57, 2013.

[14] T. Kwak and S. Moon, “A Digital Doorlock with Voice Recognition,” in *Proceedings of KIIT Spring Conference*, Chungju, vol. 2012, no. 5, pp. 345-348, 2012.

[15] J. Song, J. Kim, I. Lee and J. Bang, “The Design of Digital Door lock Using the Magnetic Field,” in *Proceedings of The Korean Institute of Electrical Engineers 2014 Fall Conference*, Korea, vol. 2014, no. 11, pp. 6-8, 2014.

[16] M. Jeon, K. Kim, I. Kim, S. Lee and J. Doh, “Design and Implementation of IoT Digital Door Lock System based on Video Communications,” in *Proceedings of KIISE winter conference*, Pyungchang, vol. 2015, no. 12, pp. 1521-1523, 2015.

[17] G. Verma and P. Tripathi, “A Digital Security System with Door Lock System Using RFID Technology,” *International Journal of Computer Applications*, vol. 5, no. 11, pp. 6-8, Aug. 2010.

황형진(Hyung-Jin Hwang)

2010.2~현재 경일대학교 컴퓨터공학과 재학
※관심분야 : IoT Application, Flying Ad Hoc Networks, Internet Application 등

김권양(Kweon-Yang Kim)

1983.2 경북대학교 전자공학과 졸업 학사
1990.2 경북대학교 컴퓨터공학과 졸업 석사
1998.2 경북대학교 컴퓨터공학과 졸업 박사
1983~1988 한국전자통신연구소
1989~현재 경일대학교 컴퓨터공학과 교수
※관심분야 : 인공지능시스템, 빅데이터 분석 및 처리 등

하일규(Il-Kyu Ha)

1992.2 영남대학교 전산공학과 학사
2003.8 영남대학교 컴퓨터공학과 박사
1992~1995 증권감독원 전산업무실 5급사무원
2002~2007, 2008~2015 영남대학교 컴퓨터공학과 강사, 객원교수, 선임연구원
2015~현재 경일대학교 컴퓨터공학과 조교수
※관심분야 : 무선센서네트워크, Body Area Networks, Flying Ad Hoc Networks 등