<u>*Araştırma Makalesi*</u>   <u>*Research Article*</u>

Security-Oriented Smart Door Lock à la Internet of Things

Tarık Kadak[1*], Serhan Özdemir[2]

[1*] İzmir Yüksek Teknoloji Enstitüsü, Mühendislik Fakültesi, Makine Mühendisliği Bölümü, İzmir, Türkiye (ORCID: 0000-0002-4344-247X), tarikkkadak@iyte.edu.tr
[2] İzmir Yüksek Teknoloji Enstitüsü, Mühendislik Fakültesi, Makine Mühendisliği Bölümü, İzmir, Türkiye, (ORCID: 0000-0003-2320-9213), serhanozdemir@iyte.edu.tr

Abstract

In this study, a framework to open a door lock with a keypad is designed. The system has a database for the authorized people who has the privilege for the access to a restricted area. Authorized individuals are permitted after keying in the respective passwords. The ID of those who access the restricted area is logged on the internet, to a Google Spread Sheet table with a time stamp. An economical wi-fi module was used for internet connection. A Solenoid is used for the locking mechanism driven by a mosfet power drive. An oled screen is also provided for the visual feedback to the users. Wi-fi card is coded in MicroPython. This card is responsible for transfering the passwords from the keypad to a web server. This web server is coded in PHP which compares the incoming passwords with the passwords in the previously generated user database, and as a result sends the wi-fi card either the name of the user who opened the door or the wrong password information. The result then is conveyed to the door lock controller. Each time this is performed, wi-fi card sends the ID of the person who opens the door or the invalid password information to an IFTTT Webhook service, and the Webhook service transfers this information to a Google Spread Sheet table with its timestamp. An administrator panel has also been created with PHP codes so that new users can also be added without dealing with the codes.

Keywords: Internet of Things, Office Security, Smart Homes, Smart Offices.

Nesnelerin İnterneti Usülü Güvenlik Odaklı Akıllı Kapı Kilidi

Öz

Bu çalışmada, bir tuş takımı ile bir kapı kilidi açmak için bir framework tasarlanmıştır. Sistem, sınırlı bir alana erişim ayrıcalığına sahip yetkili kişiler için bir veritabanına sahiptir. Yetkili kişiler ilgili şifreleri girdikten sonra onlara izin verilir. Bu bölgeye erişenlerin kimliği, zaman bilgisiyle beraber bir Google Spread Sheet tablosuna çevrimiçi olarak kaydedilir. İnternet bağlantısı için ekonomik bir wi-fi modülü kullanılmıştır. Bir MOSFET güç sürücüsü tarafından tahrik edilen kilitleme mekanizması için bir Solenoid kullanılmıştır. Kullanıcılara görsel geri bildirim için bir oled ekran da sağlanmıştır. Wi-fi kartı MicroPython ile kodlanmıştır. Bu kart, parolaları tuş takımından bir web sunucusuna aktarmaktan sorumludur. Bu web sunucusu PHP ile kodlanmıştır ve, gelen şifreleri daha önce oluşturulan kullanıcı veritabanındaki şifrelerle karşılaştırır ve sonuç olarak Wi-fi kartına kapıyı açan kullanıcının adını veya yanlış şifre bilgisini gönderir. Sonuç daha sonra kapı kilidi denetleyicisine iletilir. Bu her gerçekleştirildiğinde, wi-fi kartı kapıyı açan kişinin kimliğini veya geçersiz şifre bilgilerini bir IFTTT Webhook hizmetine gönderir ve Webhook hizmeti bu bilgileri zaman bilgisi ile birlikte bir Google Spread Sheet tablosuna aktarır. PHP kodları ile bir yönetici paneli de oluşturulmuştur, böylece kodlarla uğraşmadan yeni kullanıcılar da eklenebilir.

Anahtar Kelimeler: Nesnelerin İnterneti, Ofis Güvenliği, Akıllı Evler, Akıllı Ofisler.

* Corresponding Author: tarikkkadak@iyte.edu.tr

1. Introduction

The Internet of Things (IoT) opens up tremendous opportunities to location-based projects that maximize the ability of technologies with its processing power and sensors to provide location information. The Internet of Things revolves around increased machine-to-machine communication; it's built on cloud computing and networks of data-gathering sensors; it's mobile, virtual, and instantaneous connection; and they say it's going to make everything in our lives from streetlights to seaports "smart". (Balbin & et al., 2017)

With the advent of technology, it is hard to find such field where technology has not appeared. One of the most citable area where technology is applied is security. Door access system is one of the major concerns of home security. It has been enhanced with the days using different techniques such as, mobile application, real-time authentication system (e.g. audio and video processing), Bluetooth and other technological inventions. Later, Internet of Things (IoT) has been introduced to this field as well. (Deepty, Alam, & Islam, 2019)

The various techniques that have been proposed in the past to remotely control the home security systems especially smart locks are described in the related work section. (Singh, Kaushik, & Chitkara, 2017)

Designing smart home systems by using the Internet of Things (IoT) is one of today's trends. It is a rapidly developing sector. So, In this study, a security-oriented smart door lock à la Internet of Things was designed.

2. Components and Method

2.1. Components

2.1.1. Wi-fi Module

Different manufacturers produce different ESP cards. In this study, the NodeMCU ESP-12E card was used because the Wi-fi module was also intended to be used as a development card. A sufficient number of pins and a USB input are important advantages. It can also be coded with Micropython.

The NodeMCU ESP8266 development board comes with the ESP-12E module containing the ESP8266 chip having a Tensilica Xtensa 32-bit microprocessor. Its high processing power with in-built Wi-Fi / Bluetooth and Deep Sleep Operating features make it ideal for IoT projects.

2.1.2. Solenoid

The solenoid is the generic term for a coil of wire used as an electromagnet. The device creates a magnetic field from an electric current and uses the magnetic field to create linear motion.

The solenoid which is used needs 12V/600mA power, approximately during Operation.

2.1.3. Mosfet Power Module

MOSFET stands for Metal Oxide Semi-Conductor Field Effect Transistor and developed types of field-effect transistors (FET).

The Selonoid needs 12V / 600mA power, and the development board can provide a maximum of 3.3 V. So, another power source is needed, and a mosfet or a relay should be used for switching.

2.1.4. Membrane Keypad(3x4)

The simplest component in this study is the membrane keypad. It has 4 rows and 3 columns. Therefore, it can be controlled with 7 pins. The first 4 pins are connected to the rows and the next 3 pins are connected to the columns.

It can be understood which key is pressed by properly powering the rows and controlling which column is powering.
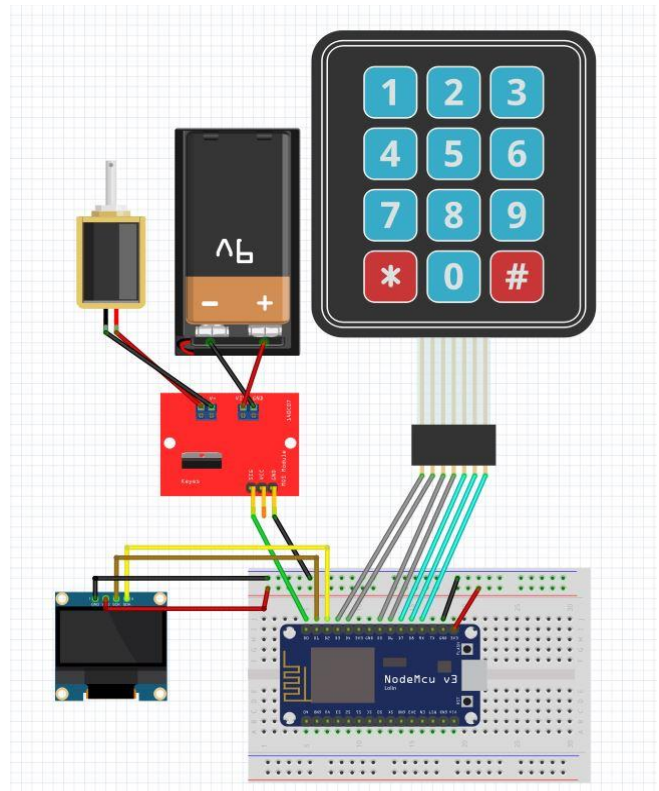

Figure 1-The Connection of Components

2.2. Methodology

Firstly, the user enters the password via the keypad. The Keypad is connected to the ESP-8266 card. The input password is read by ESP-8266. The input password is then sent to the PHP file named ENTRY CONTROL using JSON. Entry control file connects to the user database and retrieves all previously saved user IDs and passwords. It then compares the entered password with the passwords it receives from the database and sends the result back to the ESP-8266 card. Each time this occurs, ESP-8266 sends the incoming information to the IFTTT Webhook service.

Secondly, Admin encounters a PHP file called INDEX before adding a new user, where they must log in with their admin ID and password. If logged in with the correct admin ID and password, it is redirected to the PHP file named USER ADD. After entering the new User ID and password here, the data is sent to the user database. The methodology diagram is given in Figure-2.
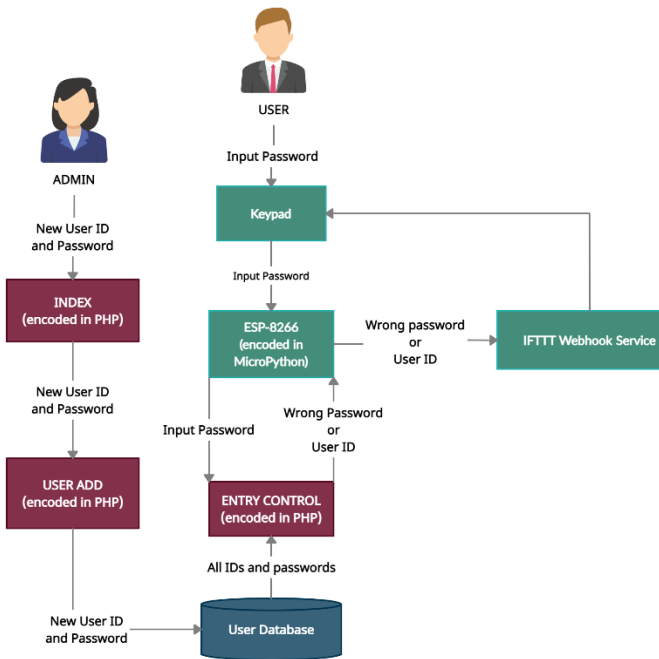
Figure 2-Methodology Diagram

2.2.1. Algorithm in ESP8266

The ESP8266 is encoded in Micropython. It shares visual output with the user via the Oled display. It connects to the WiFi with the SSID (modem ID) and password. If the wifi connection fails, the program closes. If the wifi connection is successful, a loop is initiated. And then it is directed to a subroutine called Keypad Input.

Urequest to access PHP file from ESP card the urequest.post() method and JSON (JavaScript Object Notation) were used.

request=urequest.post("url"+"api_key",".json") (MicroPython)

The flow diagram of the Keypad Input subroutine is described in detail in section 2.2.2. A 5-digit array, named B is taken from the Keypad Input subroutine each time it is pressed. If the user has not yet pressed #, it will be sent back to the beginning of the loop. If the user presses #, the last digit of array B becomes #. Input password is the first 4 digits of the B array before #. In this way, the password is obtained from the user. The Input password is sent to a subroutine named Entry Control. The Entry Control flow diagram is described in detail in section 2.2.3. . In Entry control, it compares the passwords in the user database with the input password. It then sends a variable named door value to the ESP card as 0 if an incorrect entry is made. If a correct entry is made, it sends the variable named door value as 1 and the ID of the login to the ESP card as a result of the comparison. If the door value that the ESP card receives from the Entry Control subroutine is 1, it opens the door, if it is 0, it does not open it. And in both cases, it sends the information to the IFTTT Webhook service. The flow chart of the ESP8266 card is in Figure-3. (MicroPython) (IFTTT)
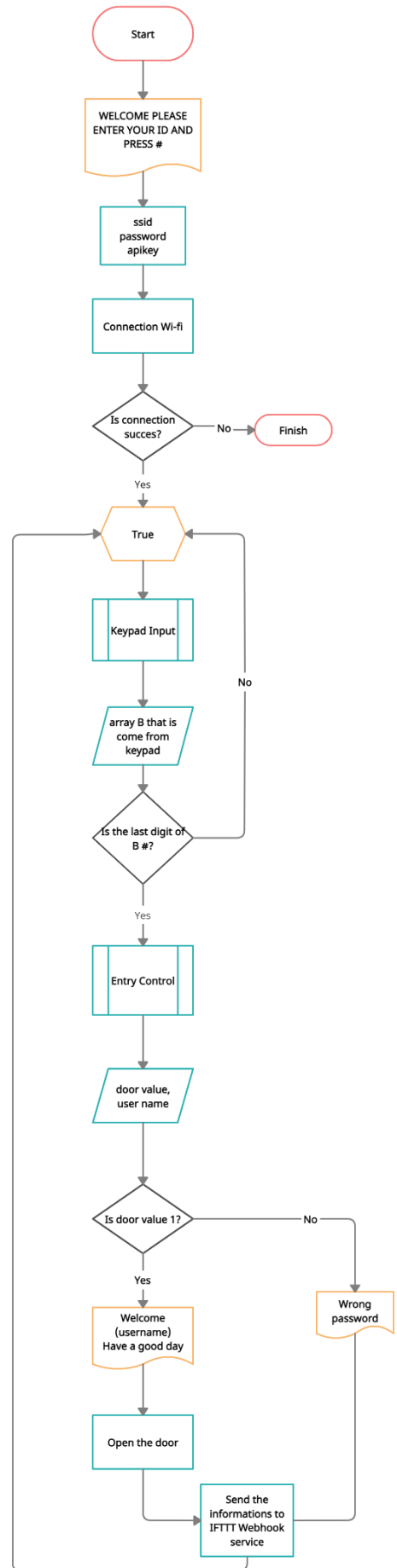
Figure 3-Flow chart of ESP8266

2.2.2. Keypad Input

Keypad subroutine is encoded in MicroPython. The purpose of the Keypad Input subroutine is to get a password from the keypad. It is simply explained how to control the keypad in Section 2.2.4.

First, the keypad matrix is written. variable c represents the column number of the pressed Key, and variable r represents the line number of the pressed key. For array B to be 5 digits, variable i is synchronized to 0 again when it is 5. So, variable i can be a maximum of 5. A 5-digit B array means that the password is also 4-digit. (When the last digit of array B is #, it means that the password has been created.) The flow chart of Keypad Input is in Figure-3.
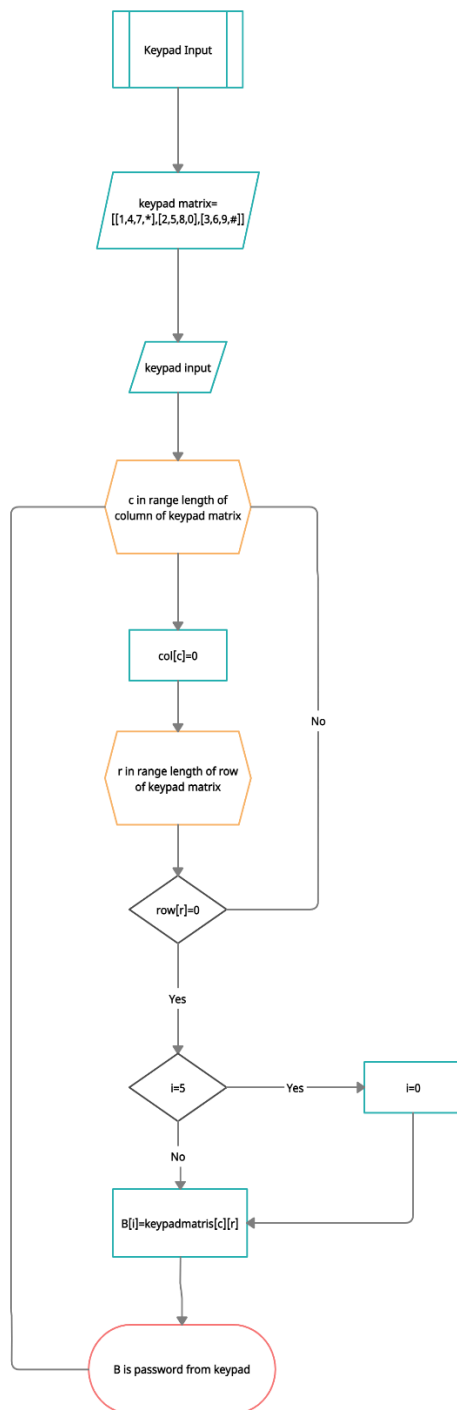
Figure 4-Flow chart of Keypad Input subroutine

2.2.3. Entry Control

Entry Control subroutine is encoded in PHP language. The purpose of the Entry Control subroutine is to take all IDs and passwords from the user database prepared with MySQL and compare them with the B array which come from the ESP card. After making this comparison, if the password is correct, it sends that person's ID and a variable named doorvalue as 1. If the password is incorrect, it sends a variable named doorvalue as 0. The flow chart of Entry Control is in Figure-3.
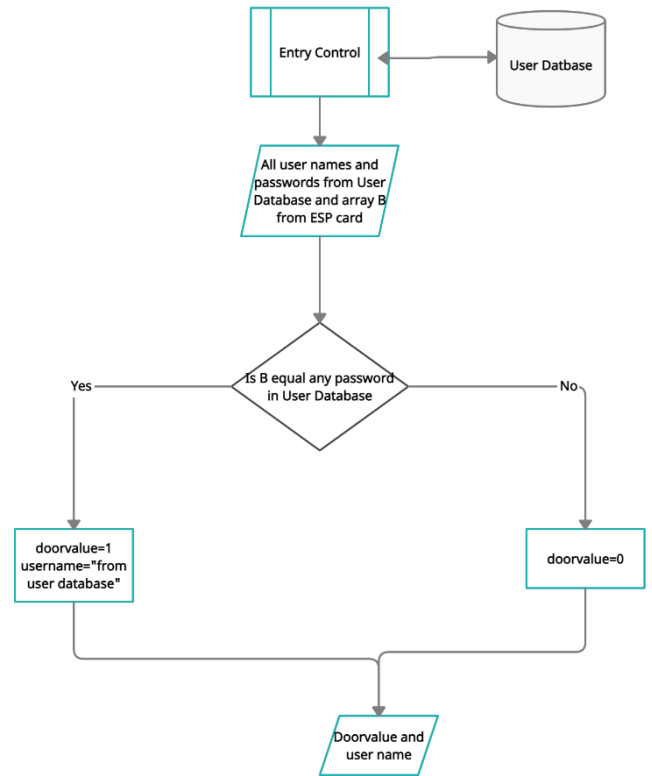
Figure 5-Flow chart of Entry Control subroutine

2.2.4. User Add and Index PHP Files

User Add and Index subroutines is encoded in PHP language. User Add file is used to add users. But in order to be able to access user Add file, you must first log in to Index file with the admin ID and password. It is connected to the Admin database and compared with the passwords entered in the Admin database. A variable named login is synchronized to 1 if the correct entry is made. Using Session, the login variable is stored on the server computer. And finally, it is redirected to the" user Add " Page. Session variables solve this problem by storing user information to be used across multiple pages (e.g., username, favorite color, etc). By default, session variables last until the user closes the browser. The reason for using Session is to still be able to read the value of the login variable as 1 when redirected to the user Add Page. In User Add File, the login variable is checked first, and if it is equal to 1, only then can admin add a new user. If the login number is missing or equal to 0, it is redirected to Index File again and is expected to enter the Admin ID and password.
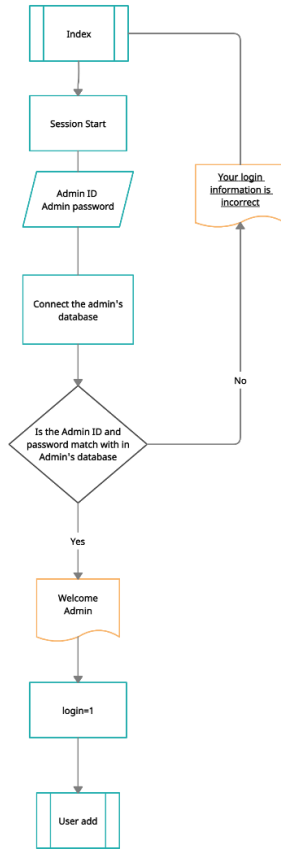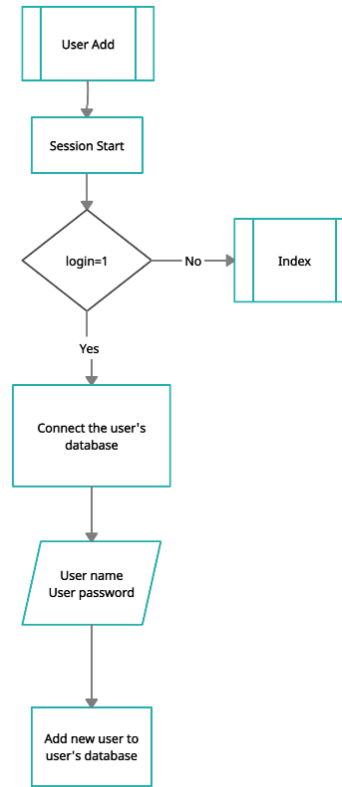
Figure 6-Flow chart of Index subroutine

Figure 7-Flow chart of User Add subroutine

3. Results and Discussion

3.1. Result

As a result, a demo of the Smart Door System was made using the components in section.2.1 and the methodology in Section.2.2.. In addition, a web interface was created with PHP files in Section.2.2.4 and an online user insertion system was prepared. Therefore, A smart door lock is designed so that users can log in with a password, save their login information online in a Google SpreadSheet file, and add an online user by admin.
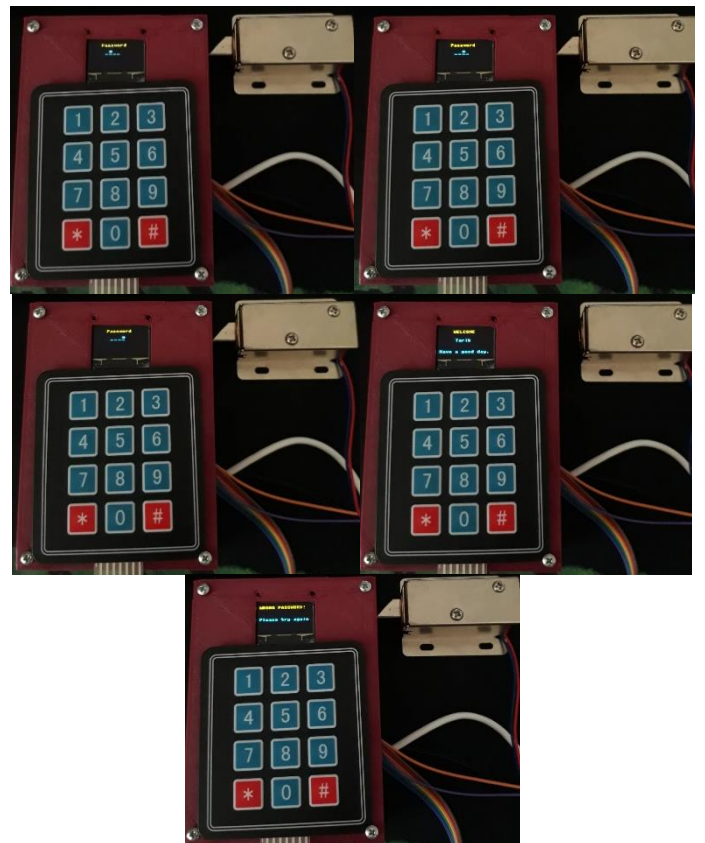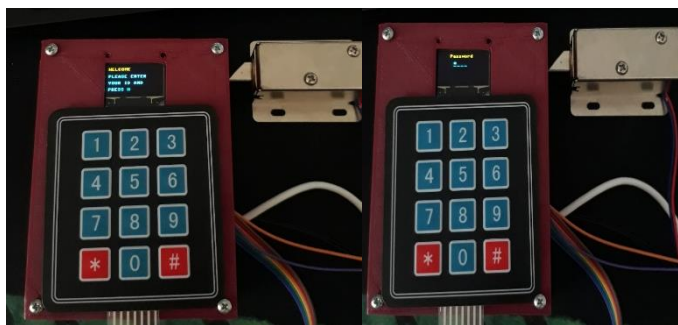
Figure 8- Some pictures of real system

Figure 9- Figure of Index File

Figure 10- Figure of Add User File

Figure 11- Figure of Admin Database

Figure 12- Figure of User Database

Figure 13-Figure of the Google SpreadSheet table

3.2. Discussion

As for the advantages of the system, its biggest advantage is cost. Besides, admin adding users online is a great advantage. In this way, Admin can access input and output information from all over the world and add new users.

To mention its disadvantages, it can be shown that currently it does not work with a battery, and the time of opening the door changes depending on the speed of the internet.

For disadvantages, the necessary recommendations for future studies are given next.

4. Conclusions and Recommendations

In this study, MicroPython, PHP, MYSQL, IFTTT services were used with minimum number of components. And a smart door lock has been designed by transferring data between them. As a result, Admin will be able to add new users from all over the world, via a web service, without entering any code. Also, this study was a good example of using different languages together. Using an ESP card as a development card without a second development card is an opportunity for minimal equipment concern. And the best way to do that is to use MicroPython. It has reduced the cost to do with PHP without adding any new hardware to add new users.

Future work could focus on the locking mechanism. Instead of a solenoid, the lock system can be driven by a mechanism that will consume less power. Also, the current model can not work without an internet connection. A model can be designed that can also work without the Internet via local connections.

5. Acknowledgements

The most important motivation for this study is the ME-587 course semester projects given at İzmir Institute of Technology. Also, thanks to Burkay Yarışanözer for his contribution to the study.

References

Balbin, J. R., & et al. (2017). Vehicle door latch with tracking and alert system using global positioning system technology and IoT based hardware control for visibility and security of assets. *2017EEE 9th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM)*, 1-5. doi:10.1109/HNICEM.2017.8269425.

Deepty, R. R., Alam, A., & Islam, M. (2019). IoT and Wi-Fi Based Door Access Control System using Mobile Application. *IEEE International Conference on Robotics, Automation, Artificial-intelligence and Internet of Things(RAAICON)*, 21-24. doi:10.1109/RAAICON48939.2019.09.

IFTTT. (2020). *ifttt.com*. Retrieved from ifttt.com/maker_webhooks: https://ifttt.com/maker_webhooks

MicroPython. (2020). *docs.micropython.org*. Retrieved from micropython.org: http://docs.micropython.org/en/latest/

Singh, S., Kaushik, A., & Chitkara, S. S. (2017). Ubiquitously controlled personalized smartlock. *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 686-691. doi:10.1109/I-SMAC.2017.8058266.