SMART DOOR LOCKING SYSTEM

Aashay Gaikwad[1], Sahil Bagwan[2], Linata Deshmukh[3], Dhankuwar Sisodiya[4]

[1]*Student, Computer, MIT College of Engineering, Maharashtra, India*
[2]*Student, Computer, MIT College of Engineering, Maharashtra, India*
[3]*Student, Computer, MIT College of Engineering, Maharashtra, India*
[4]*Student, Computer, MIT College of Engineering, Maharashtra, India*

Abstract

Modern Smart Door locks are highly prone to errors and damages making them less secure. Almost all Smart Door locks come with some passcode entry or fingerprint reader which resides outside the door making it vulnerable. This project aims at delivering the same security and reliability of a key lock mechanism making it retro and modern at the same time. As this Smart Lock operates on your phone's fingerprint reader, you do not have to rely on something which is placed outside the door. First, the user has to pair his phone with the lock via Bluetooth and can only unlock when the devices are connected and successful fingerprint authentication occurs. Currently, the range of Bluetooth is around 50 meters ,but many times it is required that the devices should be more closer for security purposes. This project uses an algorithm for estimating distance between devices connected with Bluetooth so that the user can only unlock the door when he is close to it. Also in some cases it is required to unlock the door from a remote location. To perform this action we have connected the door lock to the network via WLAN, so that the user can unlock the door from his cell phone via mobile data.

Keywords: *Smart Door Lock, Passcode Entry, Fingerprint Reader*

----------***----------

1. INTRODUCTION

All currently available smart locks come up with a device which you have to place outside of your house where you have to enter a passcode, scan your RFID or scan your finger print to unlock the door. This makes the door lock less reliable as the user has to rely on a key which is somehow present near the door. The objectives of this work are to make Smart Locking System more reliable, to develop an algorithm to estimate distance between devices connected with Bluetooth and to avail the facility of remote unlocking.

2. SYSTEM DESCRIPTION

2.1 Hardware Components

- Arduino-Yun: This board is used when designing connected devices and internet of things projects. It consists of Linux as the operating system.
- L293D IC- L293D is a typical Motor driver or Motor Driver IC which allows DC motor to drive on either direction. L293D is a 16-pin IC which can control a set of two DC motors simultaneously in any direction. It means that you can control two DC motor with a single L293D IC.
- HC-05 Bluetooth module: It is a Bluetooth module that works on serial communication.
- Power supply: 5volts

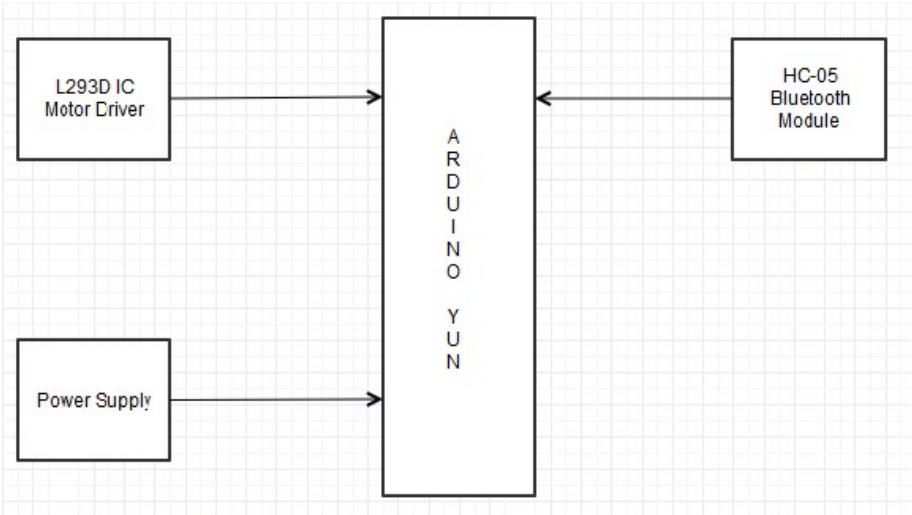

Fig. 1 – Hardware Interfacing

2.2 Software Components

XCode

Xcode is an integrated development environment (IDE) containing a suite of software development tools developed by Appe for developing software for macOS, iOS WatchOS and tv OS.

It supports source code for the programming languages C, C++,Java,AppleScript,Python,Ruby and Swift, with a variety of programming models, including but not limited to Cocoa, Carbon and Java. Third parties have added support for GNU Pascal, Free Pascal, Ada, C#, Perl and D.

Used to create the user interface for iPhone to configure and setup the lock.

Further, the user will open the same app to unlock the door.

Assembly Language

Input/Output devices are controlled using assembly language by the microcontroller.

Used to carry out locking and unlocking procedure through Stepper Motor via Arduino Yun.

MySQL Database

To save the device ID associated with the lock to unlock from remote location.

PHP

Business layer to forward the encrypted key to the lock via network.

AWS EC2

Web server to accept and forward requests to unlock the door.

3. WORKING

3.1 Phone Application

First, the user is prompted with a welcome screen for initial setup. As soon as the user taps on “Connect To a Lock”, the device will search for available locks via Bluetooth.

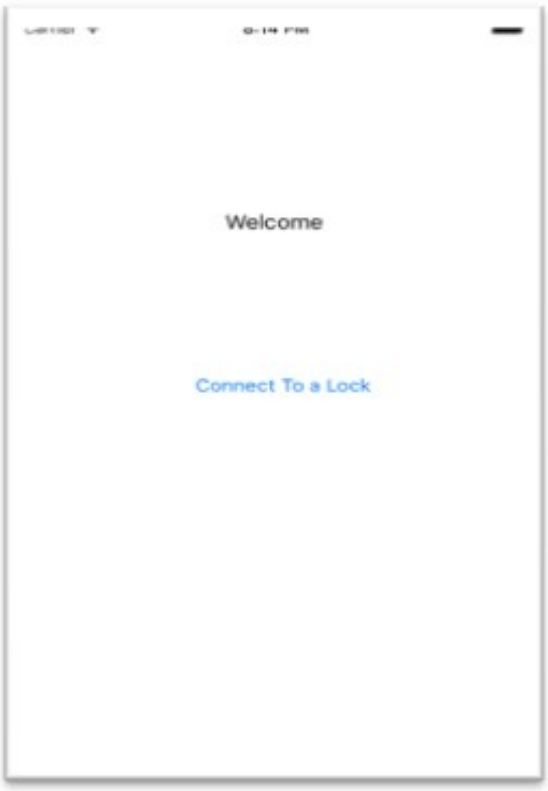

Fig 2 – Welcome Screen

Secondly, the user is prompted to enter the passcode which is hardcoded in the module for initial setup. Further, the user has to enter a name for the lock and a backup password to unlock the lock without his/herfingerprint. Now the lock is set up and ready for use.

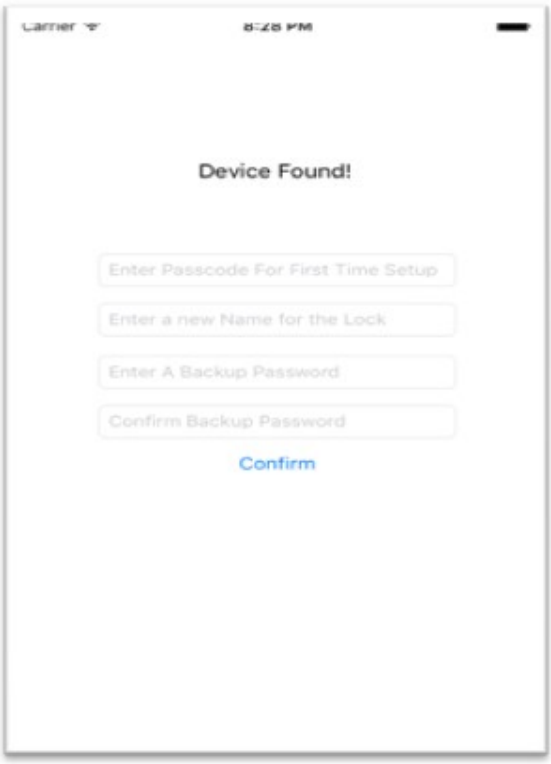

Fig 3 – Initial Setup

After the initial setup, the user will be treated with a different prompt every time he/she opens the app. The prompt will give the information about the connection with the lock, and three options to unlock the door. If the user taps "Unlock withTouchID" he will have to place his finger on the phone's finger print reader and the app will send a success signal to the lock via Bluetooth. Also, if the user is not close to the lock, the application will display a message to get near the unit and only then the door can be unlocked. Further, the user can unlock the door with a backup passcode which he had previously set up during initialization. To unlock the door from a remote location the user has to tap on "Unlock via network" option, doing so he will be prompted to scan his/her fingerprint and if the scanning is successful then send the success signal to the lock via mobile data.

Fig 4 – Unlocking the door

3.2 Lock

Once the lock is connected with the power supply it is open for pairing. Then the user has to open the app and the user will be greeted with a welcome screen if the device is not paired with the lock. Once the user taps "connect to the lock", he will be prompted to enter a key for pairing which is hardcoded in the arduino board. Furthermore, the user will have to enter a backup password. On confirmation the pairing is done and initial setup is complete.

After initial setup the user can choose from 3 options which are:
1. Unlock with Touch ID.
2. Unlock with Passcode.
3. Unlock via Network.

If the user chooses "Unlock using touch ID" the app will prompt the user to punch his fingerprint on the scanner of his phone. If fingerprint scanning is successful then the master key which is stored in the device will be encrypted by AES encryption and will be sent to the lock via Bluetooth. If the user chooses "Unlock with Passcode" then he will have to enter the passcode. After success masterkey which is stored in the device will be encrypted by AES encryption and will be sent to the lock via Bluetooth. If the user chooses "Unlock with Network" then the app will ask the user to punch his fingerprint on the scanner of his phone. If fingerprint scanning is successful then the master key which is stored in the device will be encrypted by AES encryption and will be sent to the lock via Network. Internal working of the lock: The lock will consist of a Arduino board which will be interfaced with a motor. The motor is responsible for opening the door through lever movement. When the Arduino receives a true signal from the device from which the door is being tried to open then it will make the motor rotate and the door will be open.

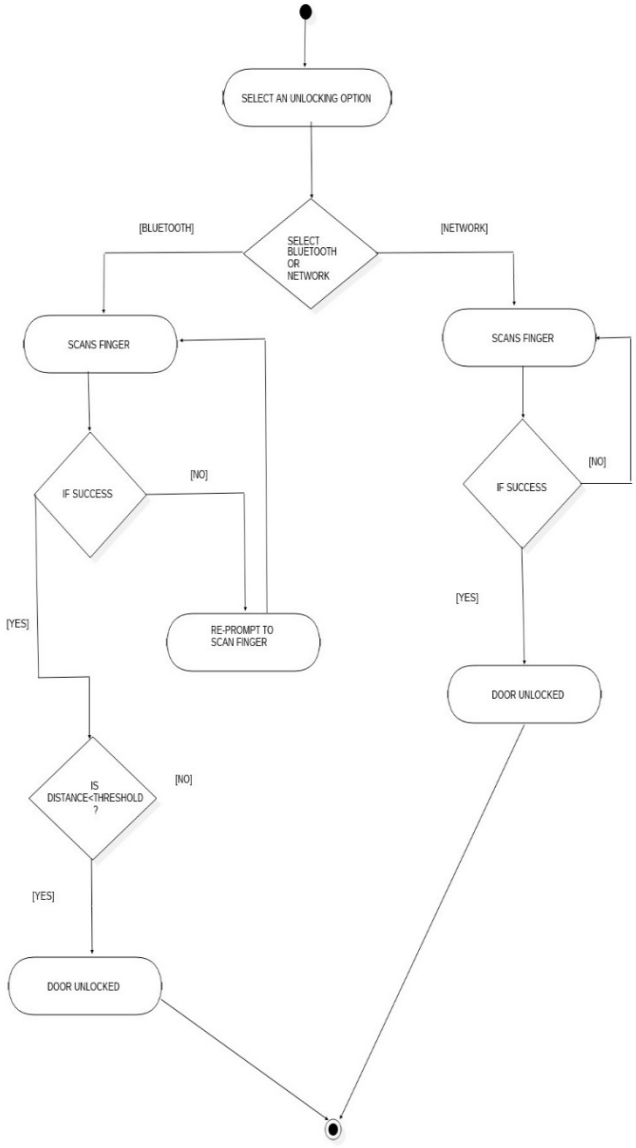

Fig 5 – Flow chart to portray the Unlocking procedure

4. EUCLEIDIAN DISTANCE ESTIMATION ALGORITHM USING BLUETOOTH

To encounter the real world scenario in this system, a Euclidean Distance correction algorithm developed from KNN is used and position calculation method is used. This is mainly due to the fact that though the average signal strength is relatively stable in the long term, its signal strength is unstable in the short term. The signal fluctuates from –1dBm to –10dBm during sampling interval. The proposed solution is the smartphone will collect data in a long term during offline data sampling and positioning, the device will calculate the average of RSS data under the MAC address. The device calculates the Euclidean distance of the RSS data and estimates the distance using following formula:

$$d(M,m,N) = (\int_1^N (M - m)^2) / N$$

M and m represents the signal strength stored in therecorded and uploaded by the smartphone respectively.

5. LAYERED ARCHITECTURE

5.1 Application Layer

To unlock the door from a remote location the user is prompted to scan his/her fingerprint, and it is verified on the device locally. The application sends an http post request to the PHP file on the AWS server which includes the device ID and the encrypted key to unlock the door.

5.2 Business Logic

It consists of a PHP5 server installed on an AWS instance. When the server receives the http post request from the application layer consisting the device ID it queries the database about the existence of that device ID for that particular lock.

Once the device ID is confirmed, the key is forwarded to the lock server.

5.3 Database

The database consists of the device IDs that are registered with the lock's configuration. The key is not stored in the database to enhance the security.

6. BENEFITS

Security: We use two layers of security
1. Military grade AES encryption for pairing the lock with phone.
2. Fingerprint scanning is done thus enhancing the security, as finger print cannot be copied.

Convenience:
1. There is no need to carry a key.
2. Unlocking mechanism is effortless for the user.
3. Interactive
4. Fast
5. Remote access to the lock.

7. FUTURE WORK

A camera can be used which gives the live stream of the person in front of the door and via the same network, the authorized user can unlock the door. Also a log of visitors can be maintained into a database

8. CONCLUSION

In this modern era of pervasive computing this work is a contribution to change the conventional locking system which has been used over centuries.

ACKNOWLEDGEMENT

We would like to thank our guide and mentor Prof. Dr. R.V. Pujeri for guiding us throughout the research and helping us in every milestone of this paper.

REFERENCES

[1]. Yankai Wang, Qingyu Yang, Guangrui Zhang, Peng Zhang: Indoor Positioning System Using Euclidean Distance Correction Algorithm with Bluetooth Low Energy Beacon
[2]. Ramsey Faragher, Robert Harle. Location Fingerprinting with Bluetooth Low Energy Beacons. DOI 10.1109/JSAC, 2015
[3]. S. Pandey, P. Agrawa, "A Survey on localization techniques for wireles network", Journal of the Chinese Institue of Engineers, vol. 29, no. 7, pp.1125-1148, 2006
[4]. F. Subhan, H. Hasbullah, "Designing of Roaming Protocol for Bluetooth Equipped Multi Agent Systems", Lecture Notes in Computer Science, vol. 5857, pp.759-769,2009
[5]. FazliSubhan, HalabiHasbullah, AzatRozyyev, Sheikh Tahir, “Indoor Positioning in Bluetooth Networks using Fingerprinting and Lateration approach”, International Conference on Information Science and Applications (ICISA), IEEE, Jeju Island, 26-29 April 2011, pp. 1-9.
[6]. Chen Guoping, Ma Yaohui, Zhang Baike, “Bluetooth indoor positioning based on fingerprinting technology”, Application of Electronic Technique,vol.39, no.3, pp.104-107, 2013[4] OpenACC Home. http://www.openacc-standard.org/.
[7]. XCode: www.apple.com/developer
[8]. HerryAzhariRangkuti, Joni WelmanSimatupang: Security Lock with DTMF Polyphonic Tone Sensor
[9]. 2-Channel Relay Module Specifications and Datasheet, Terra Electronica, 2011.
[10]. J. Hughes, J. Yan, and K. Soga, “Development of wireless sensor network using bluetooth low energy (BLE) for construction noise monitoring,” International Journal on Smart Sensing and Intelligent Systems, vol. 8, no. 2, pp. 1379-1405, June 2015.

BIOGRAPHIES

Aashay Gaikwad, Student in the final year of Computer Engineering at MIT College of Engineering Kothrud, Pune, Maharashtra, India.

Aashay Gaikwad, Student in the final year of Computer Engineering at MIT College of Engineering Kothrud, Pune, Maharashtra, India.

Linata Deshmukh, Student in the final year of Computer Engineering at MIT College of Engineering Kothrud, Pune, Maharashtra, India.

Dhankuwar Sisodiya, Student in the final year of Computer Engineering at MIT College of Engineering Kothrud, Pune, Maharashtra, India