International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

Configurable Intelligent Secures - 3FA Smart Lock

Samiran Das[1], V. Suresh[2]

[1]PG Student, Department of Computer Science and Technology, Tezpur University, Tezpur, India
[2]Associate Director, HCDC Group, CDAC, Pune, India

Abstract - *In the present world of technology and innovations, security is a major concern for all sectors including banking, private and public resources. Prevailing vulnerabilities and poor access mechanism can adversely affect security and integrity of any system. The proposed model is intended to develop a highly secure lock that can be configured according to the need of the required system. A three factor authentication model has been deployed (third factor is configurable) to make the system purely secure. The three factor authentication adds a additional layer of security to the already present two factor authentication model and therefore is hard to bypass or crack the system.*

Key Words: Internet of Things, Security, Smart lock, RFID, OTP, SMS, Raspberry Pi

1. INTRODUCTION

The proposed model is designed and developed to provide a highly secure lock based on the concepts of internet of things (IoT).

1.1 Background

With the increasing number of security issues and breaches, now a day's people focus more on how secure a product is. IoT security is of utmost significance as the consequences of security breaches in IoT devices can be devastating. A breach in a smart door lock can create dreadful situations for the owner. Even if there is a undetected breach which is not exploited but existing it will still give the product owner a phony sense of security which is ethically unacceptable.
The security issues in IoT is a ever growing problem and though considerable research work is done in this topic but there is not much sustainable work about implementations that can solve the problem.

1.2 Problem Definition

The security aspect of IoT connected devices is of higher significance. For a product owner to hold an acceptable implementation of the smart lock, we generalized the problems as follows -

1. How to setup a smart lock that is highly secure so that the breaching factor can be minimized ensuring strong privacy?

2. How to provide a user friendly interface and experience regardless of how complex the security architecture is?

3. How to develop a lock that can be configurable according to the need of any system?

4. How to provide a lock that is durable, reliable and efficient yet budget friendly?

5. How to develop a lock that can keep logs of all ethical and suspicious attempts to unlock the door?

1.3 Purpose

The purpose of the proposed system is to develop a lock that runs on three factor authentication mechanism to provide its user a highly secure way to keep their stuffs safe. The model is designed as such the third factor of authentication is configurable and can be manipulated according to the need of access system. The configurable aspect of the lock gives wide fidelity to use it any scenario where a security is the priority. The logs of all the attempts should be recorded for future investigation.

2. MARKET STUDY

The global smart lock market size was estimated at USD 559.4 million in 2016. The demand for smart locks is expected to exceed 135 million units by 2024. Rising adoption of connected home solutions and soaring need to establish connectivity across all electronic devices in users' houses as a consequence of growing penetration of smart homes are among the key trends escalating market growth.

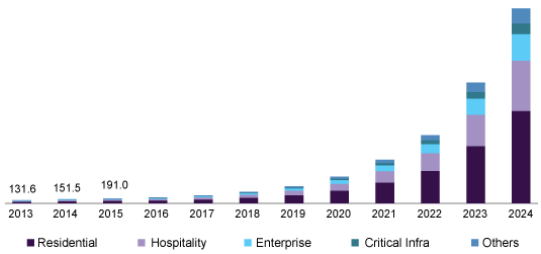

Figure 2.1 – Market of Smart Lock (2013-24)

From the above table it can be seen that the demand for smart lock is increased exponentially. Around 50% smart locks are used in residential and the rest in hospitality, enterprise, critical infrastructure etc. The smart lock

market is anticipated to witness significant opportunities for growth, particularly in cloud-based locking/unlocking management solutions, due to advent of innovative locking mechanisms through RFID cards, smart phones, tablets, and other portable devices. Adoption of sophisticated keyless access devices is relatively more conventional in mature markets, such as the U.S. and Europe, as compared to emerging economies. Lack of end-user awareness and price sensitivity are the two key roadblocks preventing widespread adoption of these devices in developing markets. However, smart locks are gradually gaining prominence across Asia Pacific, particularly in Japan and China, on account of growing level of awareness coupled with surging adoption of latest technology.

3. LITERATURE REVIEW

Many automated advanced lock has been developed over time and are used in offices, commercial places, homes etc. Some of these automated locks are based on RFID (Radio Frequency Identification) while some other uses biometric authentication or pin/password. The basic workflow of RFID is like the RFID card reader detects and validates the user accessibility. When the card is brought near the reader, it identifies the radio frequency of the card and thus verifies the key. Same goes with the biometric authentication. A user is validated by its fingerprint or facial recognition to get access.
Many researchers have come up with various speculations related to smart lock authentication mechanism for access control system.

In [4] the authors have proposed a smart door lock system which uses Bluetooth technology. The system takes the Bluetooth Mac id from users mobile and matches it to the id present in database and if it matches access will be provided by a relay driver. The owner can enroll new users in the system using a GUI based menu provided.

Rahul Satoskar, Akarsh Mishra proposed a model named smart door lock and lighting system using internet of things [5] which uses a keypad that takes password from the user to unlock the device via relay driver circuit. The lights can also be operated remotely using the proposed system.

In [6] the authors presented a system that used android smart phone to input a password that is fetched to the Bluetooth module and if matched provides access to the user. It can also automatically lock the device if it is open within stipulated time interval.

In [7] the authors proposed a system named as smart door security control system using raspberry pi which uses a camera module connected to raspberry pi that takes the picture of end user when come contact with the lock and then the picture is send to the owner via android app and then owner makes a choice whether to unlock the lock or not.

Chi-Huang Hung, Ying-Wen Bai, Je-Hong Ren proposed a model named as Design and implementation of a door lock control based on a near field communication of a smart phone [8] which uses NFC enabled smart phone to get access to the lock. When verified the specific door which is secured by this door lock control system immediately opens.

4. PROPOSED SYSTEM

The proposed three factor authentication smart lock will provide a 3 step authentication process via RFID, PIN and a random 6-digit generated OTP to the user who wants to access the lock. Below is the block and generalized diagram of the concept of the proposed system.

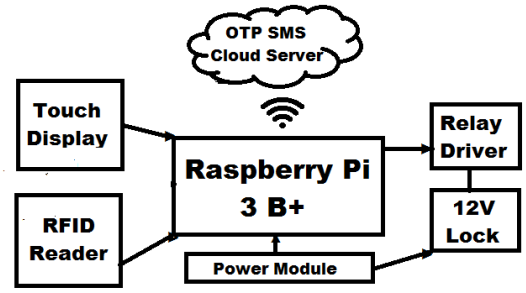

Figure 4.1 - Block Diagram of Proposed System

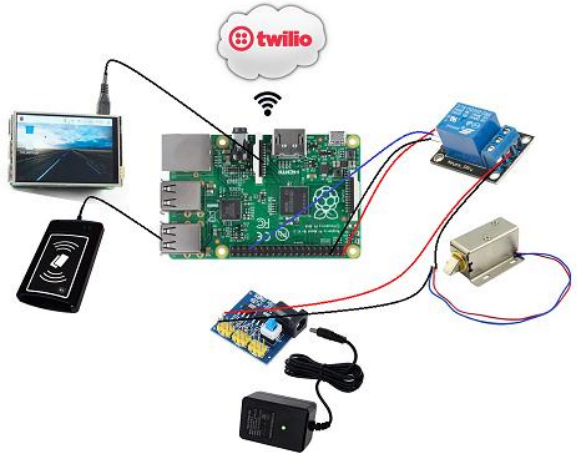

Figure 4.2 Generalized Diagram of the Proposed System

4.1 Hardware and Software Used

The model developed uses low power and pocket friendly components as described below. Rather than the hardware the software and the technology used in the project are open source besides Twilio Services (trial version).

Raspberry Pi - Raspberry Pi is a single-board micro computer made by the Raspberry Pi Foundation. It has a quad-core 1.4GHz CPU with 1GB RAM. It is a very cheap computer that runs Linux, and it also provides a set of GPIO (general purpose input/output) pins that allow you to control electronic components for physical computing and explore the Internet of Things (IoT). It has 40 pins consisting of general purpose I/O pins (GPIO), special purpose I/O pins (SPIO), 3.3V and 5.5V power source and ground pins. The proposed system uses a raspberry pi 3 B model.

Touch Screen – Touch screen is used for user interaction with the lock. A GUI based interface has been created for the same. The touch screen used in the project is 3.5 inch TFT touch display screen that is compatible with raspberry pie and fits over the GPIO pins and thus need no external connections to operate.

RFID Reader – RFID readers are used to read data from a key fob or a RFID card. A USB RFID card reader named RKI-1512 is used in the proposed system. Its operating frequency is 125 KHz and is powered by 5V power via USB.

Electric Strike - The Electric Strike is a secure electrically powered lock that can be triggered via 12V power source. The one that is used in the model is a 12 V solenoid power lock.

Relay Module - A relay is a switching device as it works to isolate or change the state of an electric circuit from one state to another. A one channel 5V DC relay has been employed for the proposed system. In the input side it has three pins via VCC, GND, and IN pin whereas the output side has also three pins namely common (COM), normally open (NO) and normally closed (NC). It needs 5V to operate. The input pin is connected to any GPIO pin of the raspberry pi to get the input signals.

DC to DC Converter - A DC to DC converter is a step down voltage converter. A DC - DC 12V to 3.3V, 5V, 12V power module multi output voltage conversion circuit is used in this project. It takes 12V as input and give 3.3V, 5V, and 12V i.e. multiple voltages as output. A 12V AC to DC adapter is used to operate the circuit.

Twilio Cloud Messaging - Twilio is a cloud communications platform as a service (CPaaS) company based in San Francisco, California. Twilio allows software developers to programmatically make and receive phone calls, send and receive text messages, and perform other communication functions using its web service APIs. In the proposed system we have used Twilio's Programmable SMS service to get OTP whenever requested by API's. The Twilio Messaging API makes it easy to send and receive SMS and MMS messages as well as query meta-data about text messages such as delivery status, associated media, and leverage tools like Copilot to manage your messages globally at scale. Twilio's Programmable SMS API helps to add robust messaging capabilities to our applications. Using this REST API, we can send and receive SMS messages, track the delivery of sent messages, and retrieve and modify message history. This REST API is served over HTTPS i.e. encrypted. Twilio's **Account SID** as the username and a generated **Auth Token** as the password is used for HTTP Basic authentication with Twilio.

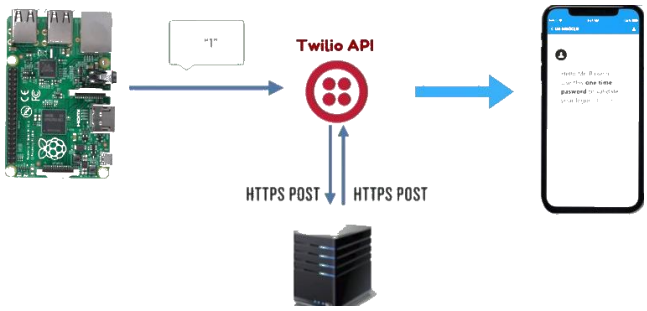

Figure 4.3 – Architecture of Twilio Cloud Communication

Apart from these, php mysql web database is used to store the logs and the credentials of different users. A user can be easily added by filling the credentials in the user table. Rest of the data like twilio sms credentials remains unchanged.

5. WORKING PRINCIPLE

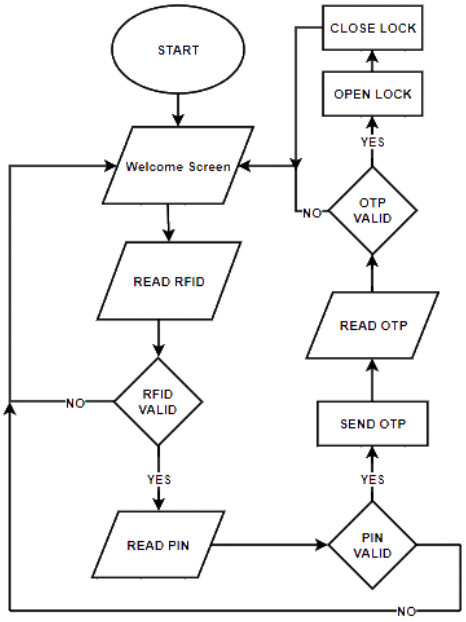

Figure 5.1 – Flow Diagram of Proposed System

The working principle of the proposed system is as follows

a) The touch screen will be showing a welcome message and is prompting user to scan their card in the reader.

b) A user will scan the RFID Card in the RFID scanner. A beep sound will verify whether the card is scanned properly or not.

c) As soon as the card is scanned properly, the system will check the database of valid users and will match the data stored in the RFID card with the stored data.

d) If the data in the RFID card does not matches with those stored in the database, the touch screen will prompt a ACCESS DENIED warning message and will revert back to welcome screen.

e) Otherwise if it matches with the stored data, the display will show the name and image of the user and will be prompting to enter the pin. If pin is not entered in 15 sec, the display will revert back to welcome screen.

f) If the pin entered by user is not matching with the stored one or in other case not valid, the display will prompt INCORRECT PIN warning message and will revert back to welcome screen.

g) If the pin entered by user matches, then the twilio sdk will trigger the api to send the programmed message generating a random digit from 100000 to 999999 i.e. a six digit OTP to the registered mobile number of that user stored in the database of user credentials. In mean time the display will now prompt the user to enter the OTP to unlock the lock.

h) The user will then receive a sms containing the OTP. If the user enters correct OTP then the lock will get unlocked and after 15 sec, it will be automatically locked again. The display will prompt a unlock message and will revert back to welcome screen. But if entered OTP is not correct or exact as received the display will prompt a INCORRECT CODE warning message and revert back to welcome screen.

Note that regardless of the fact that RFID, PIN, OTP is/are valid or invalid, all logs will be captured for all attempts successful or unsuccessful. This will help in tracing any unauthorized access and breaching attempts.

6. SYSTEM IMPLEMENTATION

The whole system requires very less space and is cheaper to implement as compared to other smart locks present in the market. The proposed system is implemented using the following components and their purpose is stated below –

Components	Purpose
Raspberry Pi	It is considered as the heart and the brain of the system. It checks the RFID, PIN and OTP data entered as an input, sends signal to the relay to activate and deactivate the lock accordingly.
Relay Module	It works as a switch that works on signal receives from raspberry pi to drive the electric lock.
DC Power Module	It satisfies the power need of the system. It provides 5V to raspberry pi and the relay module and 12V to the electric lock.
RFID Reader	It reads the data of RFID card or key fob and fetches it to raspberry pi.
TFT Touch Screen	It presents a GUI for the whole system to interact with the user as well as takes input such as PIN and OTP.

A generalized prototype of the proposed system has been designed. The snapshot of which is given below –

Figure 6.1 – Prototype of the Proposed System

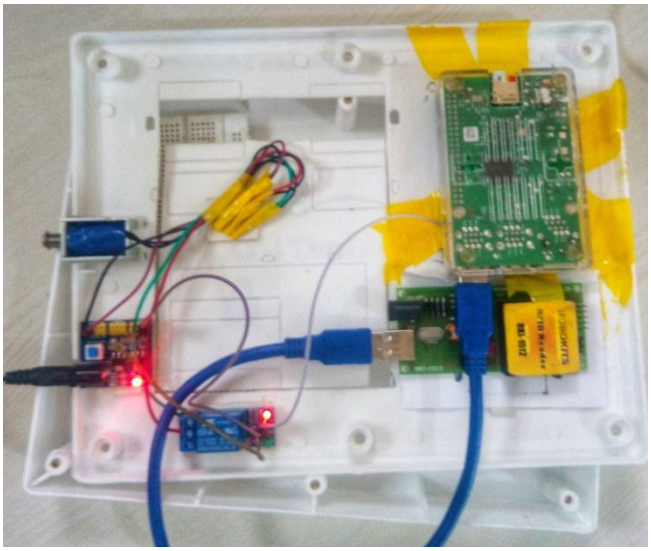

Figure 6.2 – Internal Circuitry of the Proposed System

7. CONCLUSION

Thus, the 'Configurable Intelligent Secure – 3FA Smart Lock' is a modern lock that is highly secure as it employs three step authentication which is very hard to breach and is also configurable according to the need of the system. The third factor authentication which is OTP verification in the present work can be easily modified or manipulated according to need and choice of enterprise or any individuals like biometric, gps based, voice enabled etc which makes the system flexible to use in different scenarios. Again the system requirement for the proposed model is also less thereby making it economical too. In all this lock will provide end to end security to the users while maintain the integrity of the whole system.

8. FUTURESCOPE

As the configurable factor is added to the system, therefore lots of work can be done in future to make it better. Currently the system is running by a 12V DC adapter connected to the mains but in future a rechargeable battery can be introduced inside the system to avoid power cuts and other extreme scenarios. Secondly, a multimode interface can be implemented on the present model wherein the user can browse between the types of authentication they want to use. Thirdly, a emergency response system may be implanted wherein if the lock be tampered or physically damaged, user will be able to get notification via sms or push services or in other way alarm will be triggered with sounds like barking of dogs, police siren etc.

ACKNOWLEDGEMENT

I would like to thanks Mr. Suresh V, Associate Director, HCDC Group, CDAC, Pune for his utmost support and guidance both financially and morally thought-out the project.

REFERENCES

[1] Kristoffer Djupsjö Masar Almosawi, "IoT Security Applied on a Smart Door Lock Application", KTH Royal Institute of Technology, 2018

[2] Region, And Segment Forecasts, "Smart Lock Market Size, Share & Trends Analysis Report By Type (Deadbolt, Lever Handle, Padlock), By Application (Residential, Hospitality, Enterprise, Critical Infrastructure)", Grand View Research, Inc.: Market Research Reports & Consulting, 2018

[3] Are smart locks secure? AV-TEST has the answer, https://www.techrepublic.com/article/are-smart-locks-secure-av-test-has-the-answer

[4] Jayant Dabhade, Amirush Javare, Tushar Ghayal, Ankur Shelar, Ankita Gupta, "Smart Door Lock System: Improving Home Security using Bluetooth Technology", International Journal of Computer Applications (0975 – 8887) Volume 160 – No 8, February 2017

[5] Rahul Satoskar , Akarsh Mishra, "Smart Door Lock and Lighting System using Internet of Things", International Journal of Computer Science and Information Technologies, Vol. 9 (5) , 2018, 132-135

[6] Adarsh V Patil , Akshay S, CHandanB Patgar, Sreevarsha Prakash, Mahadevaswamy, Sharath Kumar A J, "Android Based Smart Door Locking System ", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Published by, www.ijert.org NCESC - 2018 Conference Proceedings, Volume 6, Issue 13

[7] Nareshkumar R. M., Apoorva Kamat, Dnyaneshvari Shinde, "Smart Door Security Control System Using Raspberry Pi", International Journal of Innovations & Advancement in Computer Science, ISSN 2347 – 8616 Volume 6, Issue 11 November 2017

[8] Chi-Huang Hung, Ying-Wen Bai, Je-Hong Ren, "Design and implementation of a door lock control based on a near field communication of a smartphone", IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW), 2015, DOI: 10.1109/ICCE-TW.2015.7216992

[9] Bill Phillips, "The Complete Book of Locks and Locksmithing, Seventh Edition", McGraw Hill Professional, 21-Oct-2016

BIBLIOGRAPHIES

Samiran Das is a final year student of Master of Computer Application from Department of Computer Science and Engineering, School of Engineering, Tezpur University. He has done several projects on IoT and Web Development. His acute interests are Cloud Computing, Artificial Intelligence, Computer Vision, Deep Learning, Data Science and Big Data.

Suresh V is the Associate Director of HCDC group at Centre for Development of Advance Computing, Pune. He has done quality work in industrial iot with different governments and non-governments organizations.