VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

SMART OTP-BASED LOCKER

Final Document

Prof: Dr. Sathiya Kumar C.

Course: Internet of Things
Code: CSE3009

By:
Soham Faldu 19BCI0024
Vidhi Moteria 19BCE0525
Abdeali Jaroli 19BCE0190

Abstract

We are going to develop a smart locker that will have a three-tier security system for excess safety. There will be three locks and each of them secured by a different type of sensor. The top will be secured using face recognition, the middle one will be a passcode that will be sent in the form of OTP on the registered mobile number and the bottom one will be a fingerprint sensor. Using the ESP 32 camera we are going to use face detection and face recognition, using GSM SIM800l we are going to send the OTP to the registered mobile number. We have set up a database for multiple users so that OTP can be sent to that specific person. The real-time database is made on firebase and it will have user code and mobile number. So the person will have to first enter the user code then the OTP will be sent. And if anyone tries to break any of these safety locks, the buzzer will be initiated. The last security is a fingerprint sensor. So, a fingerprint is highly specific and is safer. The basic idea of this research paper is to highly increase security and make use of biometrics as a security policy because they are highly specific and it is really difficult to crack them.

Keywords: Breadboard, battery, servo motor, Buzzer, Arduino, fingerprint sensor module R307, ESP32 camera, GSM module, keypad.

1. Introduction

Today, robbery in banks, homes or at any place where a locker is situated is a big problem. Most of the conventional lockers either can be cracked by physical force or smartly by trial-and-error method. Smart lockers can be really sensitive and can alert if anyone tries to rob the banks or homes. More secure way of keeping our valuable if we digitalize the locker system also.

We are going to use OTP-based system which covers up password-based system’s vulnerability. Directly sending the OTP to registered mobile number which is more convenient. And lastly, added security of face recognition with fingerprint sensor.

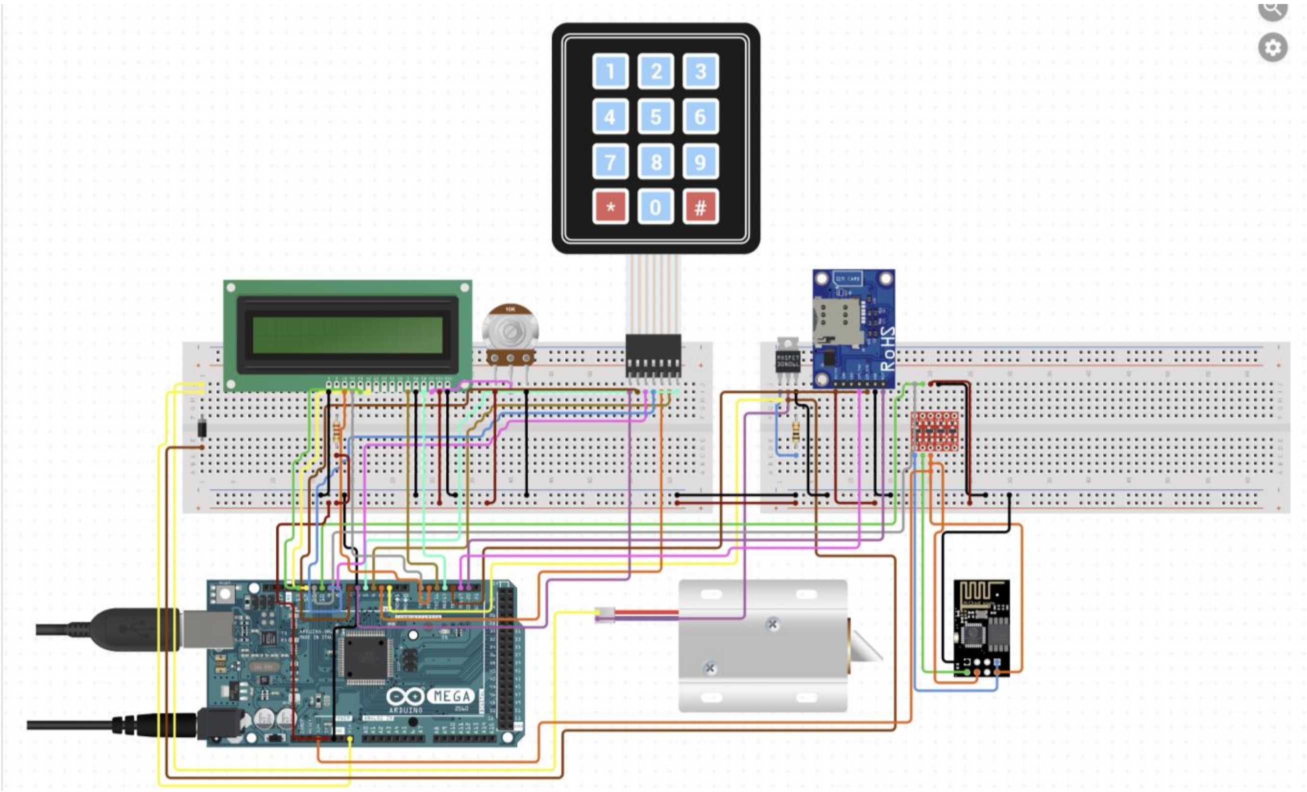
Problem Statement

We are going to make a high security vault or smart locker. In many places they use conventional lockers which can be cracked by brute-force attack. Making a locker as much secure as possible.

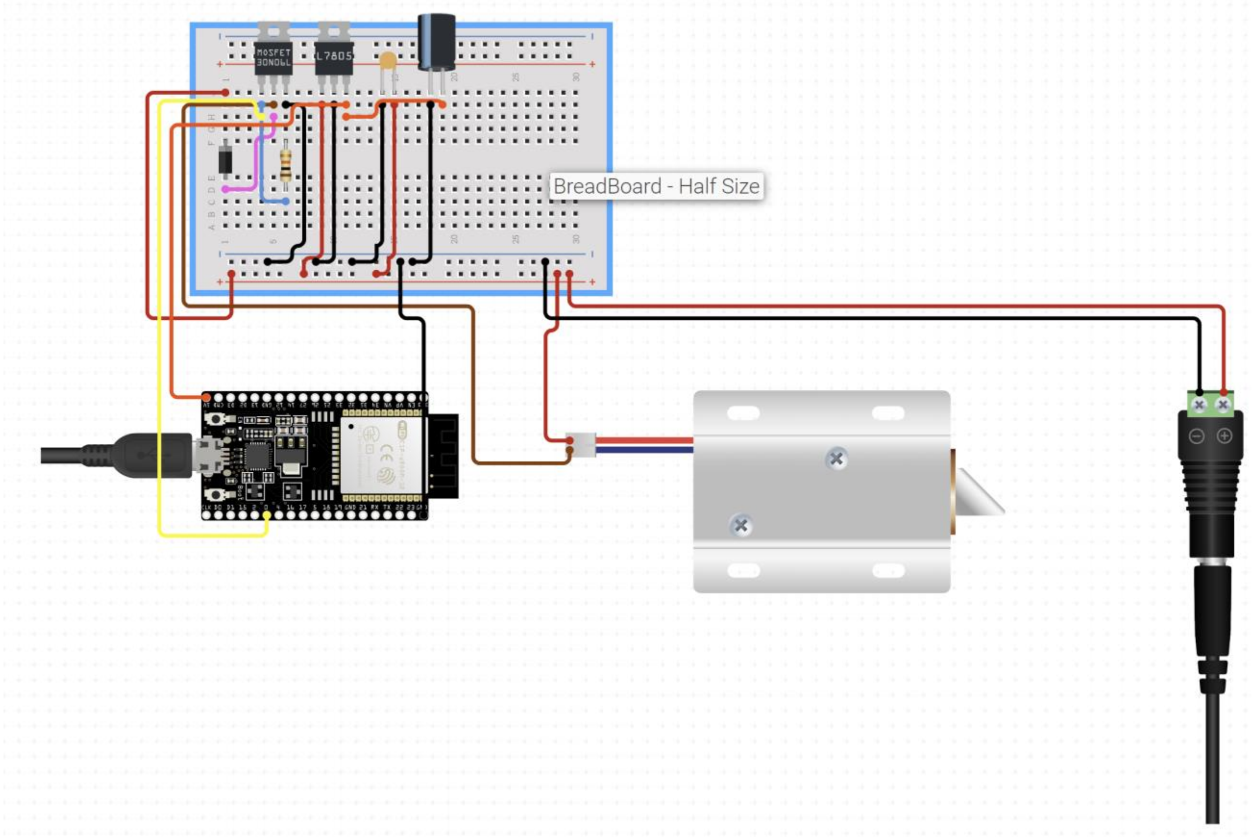
2. Architecture Diagram:

Making a smart locker with face recognition, fingerprint sensor and OTP based password.

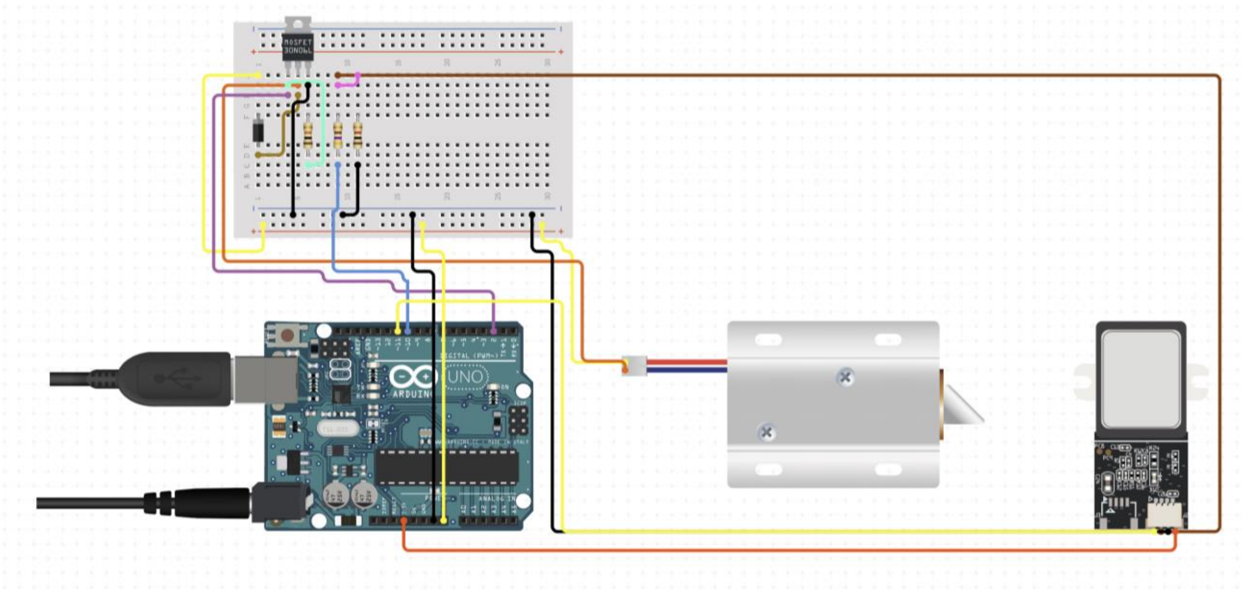
1. GSM Module, LCD, Keypad, Wi-fi module.



2. ESP 32 CAM



3. Fingerprint sensor



3. Background Study:

1. **(Base Paper) Smart Locker - IOT based Intelligent Locker with Password Protection and Face Detection Approach:** In this model they have used OTP and face recognition for security and authentication. The user has to first login in the system and ask for the OTP. Then they will get an email in return with the OTP. After entering the OTP, they will be authenticated using face recognition.

2. **IOT BASED SMART LOCKER SECURITY SYSTEM:** This model uses three step security. First you have to authenticate using password and username. Then authenticate using fingerprint. And finally receive an OTP. Enter that OTP in the system.

3. **An IOT based Smart Locker using BLE Technology:** In this model they have secured the duplicating of the digital key to the smart lockers which share their key using BLE. The keys over which are shared over the network can be cryptographically duplicated. This model defines a function known as physical unclonable function (PUF) so that if they clone the key, the lock associated with it cannot be open.

4. **LockerSwarm: An IoT-based Smart Locker System with Access Sharing:** This model is made of the lockers in any college or institution that keeps personal belongings. Losing of key is the main agenda of this model. They suggest that every locker should be opened by a unique QR code that is given to the student. So, basically using QR code as the passcode they can make it secure.

5. **Fingerprint Based Security System using GSM Module:** This paper mainly focuses on using wireless technology for security effectively. The system is SMS-based and uses biometric technology to revolutionize the standards of security. It uses a GSM Modem to send an SMS to the authorized person in case of an intrusion. The project is realized by interfacing a fingerprint sensor with an 89c51 microcontroller and a GSM Module. As the system uses GSM technology, it provides ubiquitous access to the system for security.

6. **Multilevel Security System for Automotives using RFID and Biometric Techniques:** Proposed thesis aims at securing the automotive using the technologies like Radio Frequency Identification (RFID) technology, thumb registration system and face recognition. The operational modes in this project are classified as training mode, automatic mode and manual mode. For emergency, a key insertion slot will be placed in the system with the help of which the user can insert the key. During this emergency mode of operation, the camera captures the driver's image and sends it to the owner's mobile.

7. **Cloud Computing based Intelligent Bank Locker System:** The proposed system consists of wireless switch, Raspberry pi 3, GSM and finger print scanner in order to allow only authenticated customer to open their lockers to take their accessories. If the authentication fails, the GSM automatically sends the message to the customer regarding failure of locker opening, and gives the alarm signal that makes the people in the bank to notice.

8. **Locker Opening and Closing System Using RFID, Fingerprint, Password And Gsm:** The main goal of this paper is to develop and implement a high-security locker framework using RFID, FINGERPRINT, PASSWORD, and GSM. This article discusses two main types of algorithms as well as four different sensor designs (optical, ultrasonic, passive capacitance, and active capacitance). The key advantage of RFID, FINGERPRINT, PASSWORD, and GSM over other systems is that they are more stable. RFID is a method of identifying a person or entity by transmitting a radio frequency signal. In other words, radio frequency identification (RFID) is an automated method of transmitting data over radio waves. A large range of objects can be identified, tracked, sorted, or detected using this technology.

9. **Fingerprint Verification of ATM Security System by Using Biometric and Hybridization:** The fingerprint trait was chosen because of its availability, durability, and high accuracy, according to this paper. To protect the ATM computer, a fingerprint-based biometric system can be easily implemented. When a customer places their fingerprint on the fingerprint module and then accesses the ATM to withdraw money, the machine requests the fingerprint of the user who is using the machine. It verifies/identifies fingerprints using biometrics and provides a reliable answer as to whether they are valid or not.

10. **IOT based Theft Preemption and Security System**: The paper proposes a novel security system based on Open-source cloud server thingspeak.com and a low cost esp8266 Wi-Fi module. The project includes a PIR module which constantly monitoring the Home or Work space to be monitored. When the PIR module detects an intruder, it sends a signal to the Atmega 328p microcontroller and the controller is connected to a Esp8266 wifi module and also to an alarm system. The System transmits an alert signal to the Open-source cloud which provides an alert signal on the user’s mobile phone. The system employs a second esp8266 module which is programmed to act as a web server, which allows the user to activate or deactivate the security system by means of any device with internet. The system also employs a thumb print reader rs305 which controls the opening and the closing of a safety locker door. Thus, the system uses esp8266 Wi-Fi module and atmega328p to control the security system from the user’s mobile phone by means of any device with a potential internet connection.

4. Research Findings

All the existing system and the most recent system are using password-based system along with the fingerprint sensor. The password can be really monotonous and can be hacked easily. So, we are going to cover-up that with the OTP based system. Also, one of the systems has used OTP with android app which is password protected. Now the user will not be convenient with every time entering the password to the app and then getting the OTP. So that system isn’t so user friendly. Covering that we are directly going to send SMS to the registered mobile using the GSM module. This way it will be more convenient to the user. And in any of the system they haven’t used the face recognition with the fingerprint sensor for added security. So, we are going to keep both.

5. Methodology

Technologies Used:

GSM Module: A GSM modem or GSM module is a hardware device that uses GSM mobile telephone technology to provide a data link to a remote network. From the view of the mobile phone network, they are essentially identical to an ordinary mobile phone, including the need for a SIM to identify themselves to the network. It is a wireless modem that works with a GSM wireless network and modem sends and receives data through radio waves. Like a GSM mobile phone, a GSM modem requires a SIM card from a wireless carrier in order to operate.

Wi-Fi Module: The ESP8266 Wi-Fi Module is a self-contained SOC with integrated TCP/IP protocol stack that can give any microcontroller access to your WiFi network. The ESP8266 is capable of either hosting an application or offloading all Wi-Fi networking functions from another application processor.

ESP 32 Cam Module: The ESP32-CAM is a small size, low power consumption camera module based on ESP32. It comes with an OV2640 camera and provides onboard TF card slot. The ESP32-CAM can be widely used in intelligent IoT applications such as wireless video monitoring, Wi-Fi image upload, QR identification, etc.

Fingerprint sensor: The GT511C3 is an optical Fingerprint sensor, meaning it relies on images of your fingerprint to recognize its pattern. The sensor actually has a camera inside it which takes pictures of your fingerprint and then processes these images using powerful in-built ARM Cortex M3 IC.

Firebase: Firebase is a Backend-as-a-Service (Baas). It provides developers with a variety of tools and services to help them develop quality apps, grow their user base, and earn profit. It is built on Google’s infrastructure. Firebase is categorized as a NoSQL database program, which stores data in JSON-like documents.

Solenoid lock: A solenoid door lock is a remote door locking mechanism that latches or opens by means of an electromagnetic solenoid. In most cases, the actual locking mechanism of a solenoid door lock will be identical to a conventional key-operated example.

Arduino Mega: The Arduino Mega 2560 is a microcontroller board based on the ATmega2560. It has 54 digital input/output pins (of which 15 can be used as PWM outputs), 16 analog inputs, 4 UARTs (hardware serial ports), a 16 MHz crystal oscillator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller.

TTL programmer: A device that has a TTL port provides the computer with a USB port. By connecting this converter to the computer and installing the driver program, which adds a virtual serial port to the computer ports, which is capable of working with Windows operating systems, MAC, Linux. On the output of this converter, in addition to the TXD, RXD and GND pins, the output voltage is also 5v and 3.3v.

6. Proposed model

In this project, we have made a smart locker with various steps of security as mentioned above. We have used one solenoid lock for each step of authentication here, i.e., one for fingerprint sensor, one for face-recognition camera and the last for OTP based phase. These 3 locks are used for increased security and main motive for using these locks is that, even if one lock is opened via the fingerprint recognition, other locks remain locked. Increasing the security in all possible situation.

About the arrangements of these locks in the door, we have kept the topmost lock for ESP 32 CAM, then comes the lock for OTP system, and the last for fingerprint recognition. The ESP 32 CAM circuit is kept on the top most phased so that the camera can capture the face with ease. The OTP based circuit is the most important circuit so it is kept is the middle and the whole circuit lies behind the door so that it cannot be harmed. The fingerprint sensor circuit is kept the lower most so that the sensor can be kept reachable to the user at the bottom. This our whole arrangement of the locker.

The users will be given a passcode or number so that we can connect to the database and retrieve their mobile numbers. So, if there are 4 people in a house and they want to access the locker than first we will give them a passcode (like 1,2,3,4) and in the database, corresponding to those passcodes the mobile numbers on which the OTP has to be sent will be saved. Hence, using the Realtime database for saving the details of the members who can access the locker and the numbers on which the OTP should be sent.

As we move ahead step by step, our locks will get unlocked one by one. When ESP 32 CAM will recognize the face, the first lock will get opened. Further, User 1 will enter 1 (2 for User 2 and so on) in the keypad so as to activate the OTP based system. The database will send OTP to the mobile number registered under 1 (User 1). After entering the received OTP digits, the second lock will unlock. Lastly, the fingerprint scanner will be used, and it matches then only our locker will open. Any wrong input in OTP, or the fingerprint or face is not recognized, buzzer will be activated and the locks will set back to normal.

7. Results and Discussion

Smart locker with multi-level locks is indeed a secure way. They are really convenient. There is no dilemma of handling and protecting the keys. The automatic opening and locking system, activated through smartphones and biometric readers, eliminates this dilemma.
The most secured system is fingerprint recognition because a fingerprint of one person never matches the other. Fingerprint proves to be one of the best traits providing good mismatch ratio, high accurate in terms of security and also reliable.

Talking about OTP based system, every time a different combination of numbers is sent to the registered mobile number. This increased the security and only the authenticated person will receive the OTP. If random person or a thief tries to break through, he will not receive the OTP, and in fact, inform the owner that someone is trying to unlock the locker.

Also, even if the intruder brings a duplicate fingerprint somehow, he won’t be able to open the face recognition. It is the safest method. Because the mobile can be mugged, fingerprint can be taken by some forensic means, but intruder cannot bypass face recognition. ESP 32 CAM can be used as a safe security protocol through face recognition because it easily finds an intruder.

Though this multi-tier smart locker is made keeping all the possibilities in mind, there are still some disadvantages. The most striking problem for those models operating with smartphones, is linked to the possibility of not being able to open the door when the battery of the smartphone is down. This kind of inconvenience is pretty relevant, and it would never happen with a conventional lock. As fingerprint or face biometric system is used then large data base is required. In this locker system, the user first goes through face recognition, then 4-digit code will generate through GSM on person mobile and person will enter the code by pressing key, and then places finger in finger print module. This process is a bit time consuming at initial stages.

8. Conclusion & Drawbacks

A complete smart locker with high security is completed which is nearly impossible to break. The only drawback is the cost of making the locker. It will be costly than other normal lockers. We can work on decreasing the cost further.
In terms of security, it is really durable. But it should have a battery backup because if the power source is cut then the Arduino will restart causing the solenoid switches to open of a short duration and then closing.

9. References

1. https://www.researchgate.net/publication/333085904_Smart_Locker_IOT_based_Intelligent_Locker_with_Password_Protection_and_Face_Detection_Approach
2. http://www.ijarse.com/images/fullpdf/1523727100_441IJARSE.pdf
3. https://www.ijert.org/research/an-iot-based-smart-locker-using-ble-technology-IJERTV8IS050160.pdf
4. https://ieeexplore.ieee.org/document/9071664
5. http://www.ijera.com/papers/Vol7_issue5/Part-2/F0705023134.pdf
6. https://www.researchgate.net/publication/327013771_Multilevel_Security_System_for_Automotives_using_RFID_and_Biometric_Techniques_in_LabVIEW
7. https://iopscience.iop.org/article/10.1088/1742-6596/1717/1/012020
8. https://www.ijettcs.org/Volume2Issue2/IJETTCS-2013-04-03-060.pdf
9. http://www.ijsrp.org/research-paper-1112/ijsrp-p1141.pdf
10. http://www.ijirset.com/upload/2016/march/229_IOT.pdf