**DOOR LOCK SYSTEM USING O.T.P**

Submitted in the partial fulfilment of MPMC lab

By

Abhijit Panda (B214001)

Rahul Sinha (B214042)



Department of ETC

Under the guidance of

Prof. Venkata Sridhar T.

M.Tech., PhD (Pursuing from VTU)

**List of Topics**

Chapter 1: Introduction…………………………………………..

Chapter 2: Literature Survey……………………………………

Chapter 3: Project Work………………………………………….

* Title justification
* Working Procedure
* Source code

Chapter 4: Implementation……………………………………..

Chapter 5: Conclusion……………………………………………..

* Future scope
* References

Abstract

**OTP BASED DOOR LOCK SECURITY SYSTEM**

Today people are facing more problems about security in all over world, nowadays security is the most important issue in the world. In past, research has undergone on various door lock security systems like traditional security systems which gives the signals in terms of alarm. Some door lock security systems are based on microcontroller, GSM, GPS, many sensors, software like MATLAB, PROTEUS, biometrics like face recognition Iris scanner, RFID, Smart Card, password, etc. The OTP based door lock security system is proposed to complement the drawbacks of the different security systems such as digital door-lock and mechanical door-lock based system. The proposed method does not need user’s help to get access to facility but the user must have the registered mobile phone to get the OTP. Then the OTP will be generated and sent to the user’s mobile phone when the user requests to access facility .And by entering the OTP through keypad on the door is to answer the security question ask by system. The proposed system can overcome the problems of loss or theft in conventional door lock security system. Also in the system camera is attached. Whenever the person come in front of the door then the photo will capture through camera and displays on the display in the home. Then user will open the door.

This work is on the design and construction of such a door lock with a keypad to be mounted on the door which can only access through OTP every time. Authentication claims user’s identity, and currently ID/Password based authentication is most widely used. However, there is a big problem to verify user’s identity with simple information. The password of the superfluous authentication mechanisms can overcome such drawbacks to generate a password on each time. An authentication mechanism that is able to overcome such drawbacks is one time password technology. The Raspberry Pi is the

Chapter 1

Introduction:

Security is a major issue in today’s date. With the increasing rate of thefts and bulgarities security of any place has become a concern among the public. Be it house, bank or any precious organization of national importance, a good security system must be installed.

In this 21st century we have made a remarkable progress in the field of technology. This technology can be used in order to keep ourselves and our belongings safe.

Our project focuses on use of such a technology i.e. One Time Password (O.T.P) for door lock system.

In past, research has undergone on various door lock security systems like traditional security systems which gives the signals in terms of alarm. Some door lock security systems are based on microcontroller, GSM, GPS, many sensors, software like MATLAB, PROTEUS, biometrics like face recognition Iris scanner, RFID, Smart Card, password, etc. The OTP based door lock security system is proposed to complement the drawbacks of the different security systems such as digital door-lock and mechanical door-lock based system.

A **one-time password** (**OTP**) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication; a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to *something a person has* (such as a small keyring fob device with the OTP calculator built into it, or a smartcard or specific cellphone) as well as *something a person knows* (such as a PIN).

The most important advantage that is addressed by OTPs is that, in contrast to static [passwords](https://en.wikipedia.org/wiki/Password), they are not vulnerable to [replay attacks](https://en.wikipedia.org/wiki/Replay_attack). This means that a potential intruder who manages to record an OTP that was already used to log in to a service or to conduct a transaction will not be able to abuse it, since it will no longer be valid. A second major advantage is that a user who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the *previous* session, thus reducing the [attack surface](https://en.wikipedia.org/wiki/Attack_surface) further.

OTPs have been discussed as a possible replacement for, as well as enhancer to, traditional passwords. On the downside, OTPs are difficult for human beings to memorize. Therefore, they require additional technology to work.

Chapter 2

**Literature Survey:**

Security becomes an important aspect for everything. Conventional security systems keep homeowners, and their property, safe from thieves by giving the indication in terms of alarm. This project is the next step to the existing password protected security systems because in this project special feature of one time password is added. The one time password security method is used in many cyber security processes such as online transactions or payments through debit/credit cards, etc. Following are some reasons which makes this system strong. These few characteristics make the OTP a strong authentication protocol.

After a lot of survey, we decided to use a raspberry pi i.e. a flexible embedded processor as our central processing unit. Raspberry pi is programmable with python. Python is also helpful in image processing. It has inbuilt library functions which makes it a very simple and easy language to work with. Moreover raspberry pi has a HDMI port which is connected to the screen.

G.Himaja, B.Rambabu, B.Malakonda Reddy “Providing Security for ATMs Using Digital Image Processing for Abnormal Incident Detection” has helped us understand the concept of OTPs and security systems.

Simon Monk “Programming the Raspberry Pi” helped us understand how to program the raspberry pi, interfacing hardware in the pi and basic programming of python.

**Chapter 3**

**Project Work**

The objective of the project is to set up a unique door lock system using the technology of OTP.

**Justification of Title:**

The OTP based door lock security system is proposed to complement the drawbacks of the different security systems such as a digital door-lock and mechanical door-lock based system. The proposed method does not need user’s help to get access to the facility but the user must have the registered mobile phone to get the OTP. Then the OTP will be generated and sent to the user’s mobile phone when the user requests to access facility. And by entering the OTP through keypad on the door the door will open. In case if the mobile is not available or off then the option to open the door is to answer the security question ask by system. The proposed system can overcome the problems of loss or theft in conventional door lock security system. Also in these system camera is attached, whenever the person come in front of the door then the photo will capture through camera and displays on the display in the home. Then user will open the door.

**Components used:**

**i] RASPBERRY PI:** Raspberry Pi board is a small size computer having more than enough processing speed and size which is not bigger than credit card. First of all, to work with raspberry pi, we need a list of things to get proper functioning and desired operations [10].This processor is mainly used in this system because of the HDMI port which is required for displaying images on display in home.

**ii] Display:** Two displays are used in this system, one is on the door to display the messages and another is in the home to display the image of person in front of the door.

**iii]** **Keypad:** We are using numeric keypad here, which is located on the door through which we have to enter the onetime password to open the door.

**iv] Camera:** Camera is used to capture the image of person in front of the door which displays on the display in home.

**V] Power Supply:** For every system to work the power supply is must. It is for the conversion of raw input power to a controlled or stabilized voltage or current for the operation of electronic equipment. Transformer + Rectifier + Smoothing + Regulator

**Vi] Relay:** It is used to close or open the door.

**Working Procedure:**

**STEP 1:** Initialize the system:The raspberry pi operating system is installed, the keypad and camera are interfaced. The system is given with a power supply.

**STEP 2:** Screen and Camera starts working: Text is displayed in the screen “Enter A to send OTP”.

**STEP 3:** Button is pressed to send OTP.

**STEP 4:** Camera captures the image and sends it to the e-mail. The image is captured only if the face is recognised.

**STEP 5:** OTP generates by the system. A 6-digit random number is generated.

**STEP 6:** OTP is sent to the registered mobile number via sms gateway.

**STEP 7:** OTP is entered through the keypad on the door. The buttons are noted as elements of matrix. The input is taken from keypad which is stored as a string and compared with the generated random number.

**STEP 8:** If the entered number matches with the generated random number, the motor drives and the door opens.

**STEP 9:** In case of failure, enter B through keypad then Master password will be asked by the system.

**STEP 10:** Answer the Password. The password is stored as a string. The password is then compared with the stored master password.

**STEP 11:** If the strings match, the door opens.

**BLOCK DIAGRAM**

Relay

Display

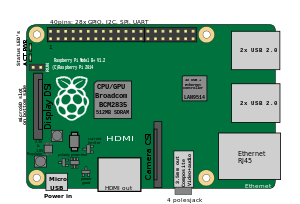
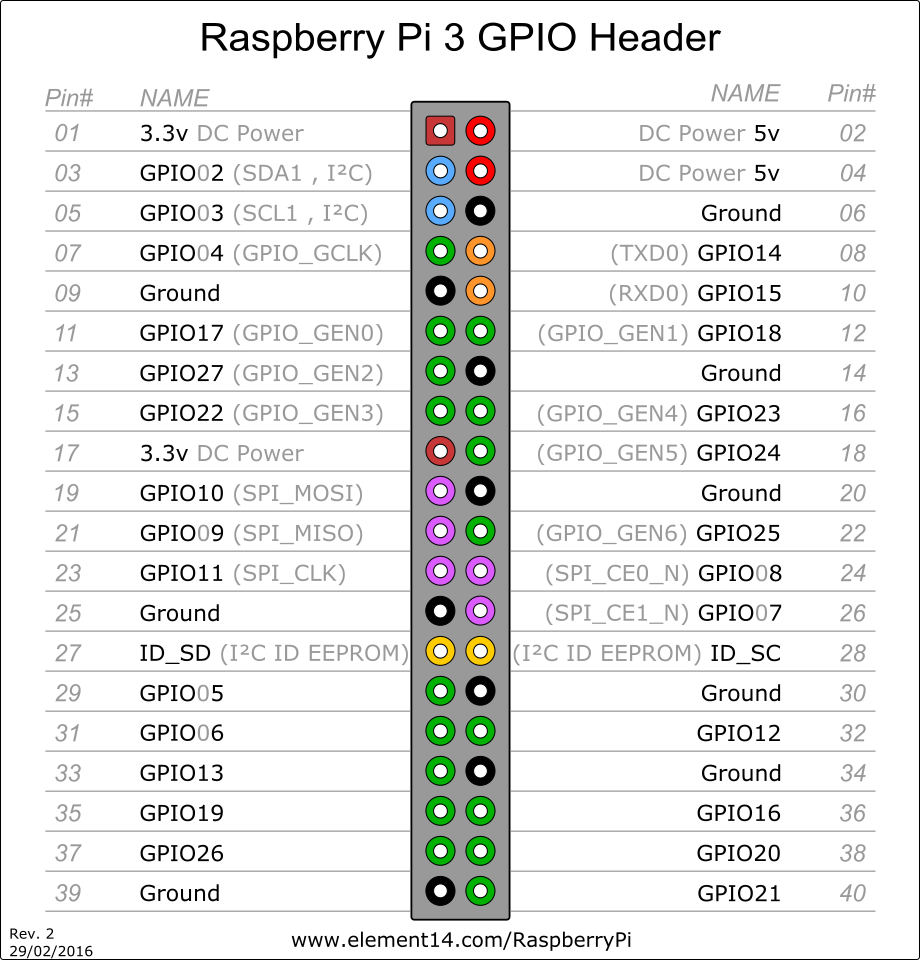
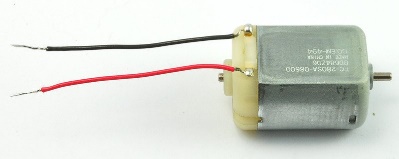
Camera

Power Supply

Raspberry pi

Keypad

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |



**SOURCE CODE**

import random

import urllib.request

import urllib.parse

import RPi.GPIO as GPIO

import time

import numpy as np

import cv2

import smtplib

import os

# Here are the email package modules we'll need

from email.mime.image import MIMEImage

from email.mime.multipart import MIMEMultipart

GPIO.setmode(GPIO.BOARD)

MATRIX = [ [1,2,3,'A'],

[4,5,6,'B'],

[7,8,9,'C'],

['\*',0,'#','D'] ]

COL = [15,13,11,7]

ROW = [22,18,16,12]

MATCH\_OTP=""

MASTER\_PASS="12345678"

for j in range(4):

GPIO.setup(COL[j], GPIO.OUT)

GPIO.output(COL[j], 1)

for i in range(4):

GPIO.setup(ROW[i], GPIO.IN, pull\_up\_down = GPIO.PUD\_UP)

def sendsms(otp):

username = 'rahsnh@gmail.com:kevinmitnick'

sender = 'TEST SMS'

numbers = '8763321018'

message = 'Beware! Only Fraudster will ask your One Time Password(OTP) over phone.use OTP %s.Do not share it with any one'%otp

values = {'user' : username,

'senderID' : sender,

'receipientno' : numbers,

'msgtxt' : message

}

url = "http://api.mVaayoo.com/mvaayooapi/MessageCompose"

data = urllib.parse.urlencode(values)

data = data.encode('utf-8')

req = urllib.request.Request(url,data)

print ('\nAttempt to send SMS ...')

status = 'Status=0'

response = urllib.request.urlopen(req)

response\_url = response.read()

print(response\_url,'\n')

def sendMail():

# Create the container (outer) email message.

msg = MIMEMultipart()

msg['Subject'] = 'DOOR LOCK SYSTEM-FACE DETECTED'

# me == the sender's email address

# family = the list of all recipients' email addresses

msg['From'] = 'rahsnh@gmail.com'

msg['To'] = 'rahsnh@hotmail.com'

msg.preamble = 'DOOR LOCK SYSTEM'

# Assume we know that the image files are all in PNG format

# Open the files in binary mode. Let the MIMEImage class automatically

# guess the specific image type.

img\_data = open('facedetect.png', 'rb')

image = MIMEImage(img\_data.read())

msg.attach(image)

# Send the email via our own SMTP server.

print("connecting")

try:

s = smtplib.SMTP('smtp.gmail.com', '587')

s.ehlo()

s.starttls()

s.login('rahsnh@gmail.com', 'kevinmitnick')

print("connected")

s.send\_message(msg)

print("Image Sent")

s.quit()

except:

print("Unable to send the email. Error: ", sys.exc\_info()[0])

raise

# FACE DETECTION

def face\_detect():

#https://github.com/Itseez/opencv/blob/master/data/haarcascades/haarcascade\_frontalface\_default.xml

face\_cascade = cv2.CascadeClassifier('/home/pi/opencv-3.1.0/data/haarcascades/haarcascade\_frontalface\_default.xml')

cap = cv2.VideoCapture(0)

cap.set(cv2.CAP\_PROP\_FRAME\_WIDTH, 640)

cap.set(cv2.CAP\_PROP\_FRAME\_HEIGHT, 360)

while 1:

ret, img = cap.read()

gray = cv2.cvtColor(img, cv2.COLOR\_BGR2GRAY)

faces = face\_cascade.detectMultiScale(gray, 1.3, 5)

for (x,y,w,h) in faces:

cv2.rectangle(img,(x,y),(x+w,y+h),(255,0,0),2)

cv2.imshow('img',img)

k = cv2.waitKey(30) & 0xff

if k == 27 or len(faces)>0:

cv2.imwrite('facedetect.png',img)

cap.release()

cv2.destroyAllWindows()

sendMail()

break

def random\_otp():

otp = random.randrange(100000,1000000,3)

face\_detect()

# sendsms(otp)

global MATCH\_OTP

otp = str(otp)

print (otp)

MATCH\_OTP=otp

return check\_otp(6)

def master\_pass():

return check\_otp(8)

def check\_otp(range\_digit):

flag = 0

option = 0

ctr = 0

global MATCH\_OTP

st=""

if range\_digit == 6:

print("ENTER 6 DIGIT OTP")

option = 0

else:

print("ENTER MASTER PASSWORD")

option = 1

while (ctr<3):

for c in range(range\_digit):

flag = 0

while(True):

if flag==1:

break

for j in range(4):

GPIO.output(COL[j],0)

for i in range(4):

if GPIO.input(ROW[i]) == 0:

print (MATRIX[i][j],end="",flush=True)

time.sleep(0.2)

while(GPIO.input(ROW[i]) == 0):

pass

if MATRIX[i][j]=='A':

return 0

st = st+str(MATRIX[i][j])

flag=1

GPIO.output(COL[j],1)

if c==5 and option==0:

if st==MATCH\_OTP:

print('\n\nOTP MATCHED,DOOR OPENED')

MATCH\_OTP=""

return 1

else:

print("\n\nINCORRECT OTP,RETRY AGAIN OR PRESS 'A' TO EXIT")

st=""

ctr=ctr+1

if c==7 and option==1:

if st==MASTER\_PASS:

print('\n\nPASSWORD MATCHED,DOOR OPENED')

return 1

else:

print("\n\nINCORRECT PASSWORD,RETRY AGAIN OR PRESS 'A' TO EXIT")

st=""

ctr=ctr+1

return 0

def loopover(flag):

try:

if flag==1:

print("\nPRESS 'A' TO SEND OTP OR 'B' TO ENTER MASTER PASSWORD")

else:

print("\nPRESS 'D' TO CLOSE DOOR")

while(True):

for j in range(4):

GPIO.output(COL[j],0)

for i in range(4):

if GPIO.input(ROW[i]) == 0:

print (MATRIX[i][j])

time.sleep(0.2)

while(GPIO.input(ROW[i]) == 0):

pass

if MATRIX[i][j]=='A' and flag==1:

state = random\_otp()

if state==0:

loopover(1)

else:

print("\nPRESS 'D' TO CLOSE DOOR")

flag = 0

elif MATRIX[i][j]=='B' and flag==1:

state = master\_pass()

if state==0:

loopover(1)

else:

print("\nPRESS 'D' TO CLOSE DOOR")

flag = 0

elif MATRIX[i][j]=='D' and flag==0:

loopover(1)

else:

if flag==1:

print("\nPRESS 'A' TO SEND OTP")

else:

loopover(0)

GPIO.output(COL[j],1)

except KeyboardInterupt:

GPIO.cleanup()

loopover(1)

**Chapter 4**

**Implementation:**

How the OTP door lock system works

* The system is installed in a door.
* When a person comes to open the door, he sees a text written “press A to send OTP”.
* When the button is pressed, the OTP is sent to the registered phone number.
* Also the camera captures the image and the image is sent to the registered email.
* The received OTP is entered.
* If the OTP matches, the door opens.
* In case of network failure, owner can enter the master password.

**Chapter 5**

**CONCLUSION**

With the development of digital technology, many services using OTP have been developed. We have implemented a door lock security system using OTP. But it observed that this system is most secure than currently available many systems based on card recognition, biometric recognition, password based etc. Also the installation cost is low. It is easy to operate and more secure for multi users. The problem of loss or theft which may occurs sometimes in available systems were solved by using OTP value on user’s mobile phone in our proposed system.

**FUTURE SCOPE**

In future this system may also develop with image processing or biometric recognition such as face recognition or fingerprint recognition etc. for the more additional security with the current security system. This system can not only be used for home door locking, but also can be used as security system in bank lockers, museums and other places which require high security system.

**REFERENCES**

**Book references**  
[1] G.Himaja, B.Rambabu, B.Malakonda Reddy “Providing Security for ATMs Using Digital Image Processing for Abnormal Incident Detection” ,International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE) ,Volume 2, Issue 4, April 2013.  
[2] Ushie James Ogri, DonatusEnangBasseyOkwong, AkaisoEtim“DESIGN AND CONSTRUCTION OF DOORLOCKING SECURITY SYSTEM USING GSM” ,International Journal Of Engineering And Computer Science ISSN:2319-7242, Volume 2 Issue 7 (July 2013).

**Web References**

<https://github.com/opencv/opencv> open cv library for face detection.

#https://github.com/Itseez/opencv/blob/master/data/haarcascades/haarcascade\_frontalface\_default.xml : face database.