https://doi.org/10.31871/IJNTR.7.5.3
International Journal of New Technology and Research (IJNTR)
ISSN: 2454-4116, Volume-5, Issue-6, June 2019 Pages 11-15

QR Code based Advanced Digital Locking System using Raspberry Pi

Bhargavi Kavalanekar, Poorva Sankhe, Nikita Rathiwadekar, Umesh Mahind

***Abstract*—In recent years, owing to the proliferation of Internet of things, homes and offices square measure being translated into good homes and offices. The paper presents an epitome of sensible door lock system which may be accustomed enhance the safety. Door locks measure a standard prevalence in our everyday lives. Yet, we tend to still trust ancient doorknobs, that use physical keys that brings with it several issues like key duplication from photos and lock-picking. The focus being security, the primary layer is the alphanumeric key security, and the next layer involves the QR code technology. QR is one of the most secure way to ensure security as it can generate a new code for each new data provided. It will be extremely helpful in tracking the number of individuals trying to access the system. The automation system includes Raspberry Pi equipped with camera and an android mobile phone. This project aims to make a door lock system as an improved alternative that accepts QR codes for the door lockup system.**

***Index Terms*—Alphanumeric key security, QR code technology, Raspberry Pi.**

I. Introduction

Over the years, the house setting has modified dramatically and most likely its one in every of the environments most full of technological advancements. With home instrumentality and tools obtaining smarter each day, its currently experiencing a serious transformation into what is currently being remarked as a sensible home. Despite of these developments, in several of homes we discover physical lock. With the new technologies, the safety of a door lockup system may be augmented by a system by incorporating cost-efficient technological solutions combined with the capabilities of smartphones and IoT solutions that area unit simply accessible within the market. One in every of these devices that simply accessible and is employed within the style of applications is that the tiny, low price laptop, Raspberry Pi, Once connected to a camera, we will produce a strong security system. The system is not meant to whole replace the task physical lock however meant to boost the safety. Currently, the most technique of limiting entry to sure individuals involves the employment of physical keys.

Bhargavi Kavalanekar, Department of Electronics and Communication, Usha Mittal Institute of Technology, S.N.D.T Women's University, Mumbai, India
Poorva Sankhe, Department of Electronics and Communication, Usha Mittal Institute of Technology, S.N.D.T Women's University, Mumbai, India
Nikita Rathiwadekar, Department of Electronics and Communication, Usha Mittal Institute of Technology, S.N.D.T Women's University, Mumbai, India
Umesh Mahind, Department of Electronics and Communication, Usha Mittal Institute of Technology, S.N.D.T Women's University, Mumbai, India

Physical keys carry with them a good range of security issues; among them the danger of physical loss, inventory trailing and lock-picking. Hence, the projected system offers.

an answer through the employment of QR codes as a way of authentication. QR codes area unit simply made, and area unit low price compared to creating a replacement physical key. They will even be simply tracked digitally making certain system up so far access log of individuals getting into and exiting. Any compromised QR code are often simply deleted or disabled. The objectives of this project are: - to analyze and analyze the necessities of a fast to use, QR code-based door lock. Using and develop the system primarily victimization and using device and a Raspberry Pi.

II. Literature Survey

In this proposed system [1] a security and vigilance system which consist of smart mirror using Raspberry Pi. The have designed system can take three modes of input Voice, Touch, Mobile commands. The Yolo Technique with Open CV (Computer Vision) for object detection is used for the detection of the Intrusion at Human. The You only look once (Yolo) is a machine learning concept for detection of object hence it works faster. But the cost of the hardware components is high, and their durability is low. Also, the Raspberry Pi used in this proposed system is having limited capability in terms of memory and processing. In this [2] a security system using the unique id fingerprint authentication to secure the car from unauthorized people. They have placed the fingerprint scanner at the place of the car door locking system to lock and unlock the doors in place of the conventional door locking system which will give more protection to the car owner. They have also developed other indication systems by using the GSM module to send the message to the car owner's mobile.
In this proposed system [3] it uses three factors for security. First is the alphanumeric password then the graphical password and question based. First security check will be the alphanumeric password which will be during the time of registration for that account. In alphanumeric system, they have applied AES Algorithm. Also, they have utilized random key generator that was created. The system requires more memory to store necessary information. And it requires additional time to login. It provides an overview of a prototype focusing on controlling lights and fans referred as Home Automation and providing Smart security by sending a capture damage through an E-mail to the owner using internet when an object is detected. The used all types of sensors which lead to an expensive structure of model that was proposed [4]. Also, the utilization of Arduino UNO and Node MCU was observed.

In this proposed system [5] Intelligent surveillance system that continuously monitors the targeted area and detects motion in each frame. This is achieved by using real time video processing using open CV (computer vision/machine vision) technology. Coming to the limitation, this system is developed specifically in a way that each time motion is detected it will send a message and video even its not that serious. It specifies [6] a door access and monitoring control system which consist of different stages – detecting by keypad and camera pi user, fetching user id, verification. Both NFC, RFID can be used in door security system. Implementation cost and availability of supply to hardware requirements was different than expected.

III. Methodology

RASPBERRY PI The Raspberry Pi 3 – Roburin's most recent offering is the Raspberry Pi Model B Original quad-core 1.2GHz 64Bit SoC with onboard Wi-Fi and Bluetooth. The Raspberry Pi 3 – Model B Original is a third-generation product with the same basic board format as other Raspberry Pi modules, but with a faster 1.2GHz 64Bit SoC and integrated Wi-Fi and Bluetooth. The Raspberry Pi 3 Model B ARMv8 w/1GB RAM has all the previous models' features, but with twice the RAM and a slightly faster processor. In two ways, the Pi3 has been improved. The first is a quad-core Broadcom BCM2837 64-bit ARMv8 processor from the next generation. This processor can run at speeds of up to 1.2GHz, which is faster than the Pi 2's 900MHz. The inclusion of a built-in BCM43143 Wi-Fi chip is the second update, enabling the Pi 3 to go wireless without any extra peripherals. Wi-Fi adapters will no longer be available. The Raspberry Pi 3 is also an outstanding IoT solution thanks to its onboard Bluetooth Low Energy (BLE).

HARDWARE SPECIFICATIONS:
- Intel processor i3 and above
- 4 GB RAM
- 256 GB hard disk
- Web camera

SOFTWARE REQUIREMENTS:
- Python
- Open CV Framework
- Windows Operating System

IV. Proposed System

In this paper the goal is to develop a framework that allows users to gain access only when they are approved. The system consists of a main layer, which is the alphanumeric key layer, which will be used as the system's input from the cell phone. After the primary layer has been tested, the user will be given a QR code to display to the camera to gain entry. Upon the user's arrival, a data entry is made into the database through a server designed to keep the device and the application in sync. The server serves as a contact hub between the User App and the Raspberry Pi with camera. Raspberry Pi board Broadcom BCM2837 quadcore ARM cortex A5340 pin GPIO header, 1.2 GHz CPU, 1 GB RAM, 10/100 Ethernet port, Broadcom 1V video core GPU, Bluetooth 4.1, micro-SD storage. The 5MP Omni Vision 5647 Camera Module is a custom-designed Raspberry Pi add-on that connects to the board through one of the two small sockets on the upper surface. This interface makes use of the CSI interface, which was created specifically for connecting to cameras. Client and professional applications make HTTP requests to the server and then utilize the response to get information. The singleton's attribute URL is used to describe the server URL. In addition, the Raspberry Pi makes an HTTP request to the server. It was agreed to merge the customer and technical applications because they have many common services. On the database, each computer can only add, update, or request data. The POST request method is used to submit the results. The attribute" request" is a number that corresponds to a particular request in each request. For example, the request value for adding a new user to the database is 1. In a POST request, user information data is given, and if an individual is added, 1 is returned; otherwise, 0. The second request is for a password. The email address and password are sent by the application. If the password matches the one stored in the database, the server sends the user data; otherwise, it returns 0. The individual ID and pin are used to control access. This data is sent to add one to the database with the request number 6. The server responds with a 1 if all went well or a 0 if everything went wrong. The individual ID and pin are sent to the server with the request value after decrypting the QR file. Person, ID, and pin are the three entities that make up the data. When and who attempted to access the system was registered.

V. Basic Block Diagram

The figure no 1 provides the basic overview of the system we have implemented. This paper consists of two sections software and hardware. Software part consists of two layers of security and hardware consist implementation of QR on Raspberry pie. The system consists of a primary layer, that is the alphanumeric key layer which will be provided as the input from the mobile phone to the system. The communication between the device and the system will happen through the communication protocol which will be Wi-Fi. The secondary layer of the system is the dynamic QR scanning. The freshly updated/generated QR code will be scanned through a camera attached to the device which will then be provided to the raspberry pie for verification. It will then process the data which is needed to be recheck or verify the received data. Upon verifying the data entry of both the layers, the raspberry PC will send out an execution signal to the security/mechanical. And the lock will then grant or deny access based on the signal received.

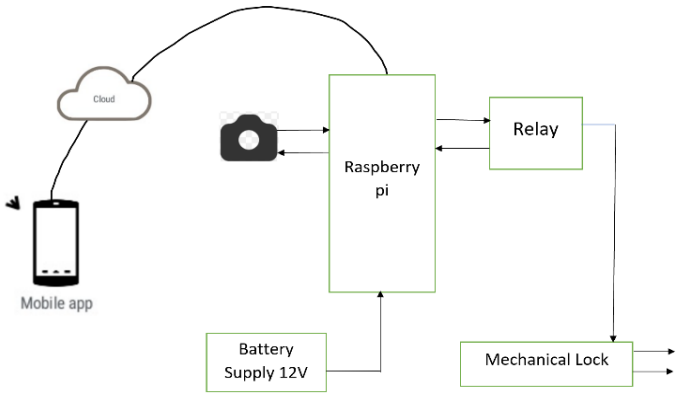

Fig. 1. Basic block diagram of security system.

VI. IMPLEMENTATION

A. *Software*

The implementation of the software is done in Android studio and database is maintained in SQL Server Management Studio.

1) Login Page-

The login part which consists of the email id and password. The email id should be a valid email id in the form of '.com' mostly importantly it should be the registered email id so that the person can the login and generate the OTP. Whenever the user will login they will be assigned with an unique id. Since the unique id is assigned only once that is during login, thus unique id will be same even if OTP changes. A unique id will be assigned to them with respect to that email id so that whenever the person tries to login it will be referred to identify that person. After that the OTP is generated dynamically. Here the OTP is an dynamic OTP, it can be different at different times but the id is unique which will be assigned during login . If the user is not registered one then first they have to signup.

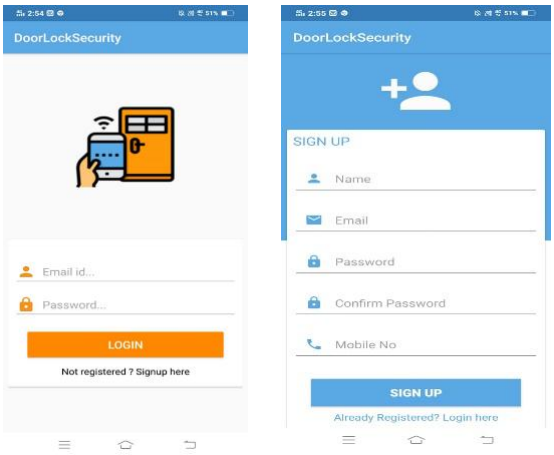

Fig. 2 Login and Signup Page

2) Sign up page: -

In sign up pages we have created 5validations that is name, email, password, confirm password, and mobile no. The email id should be in .com format. For password, the password should be of minimum 6 characters for strong security, if the password is not consisting 6 characters, then the alert box will be reflected saying "password should consist at least 6 characters". After completing the password part there will be one more option of confirm password. If both the passwords are not similar, then again, we will be getting an alert box. For entering the mobile no., the mobile no. must start from 6 to 9 as per Indian call list, the total length should be of 9 characters and 0 – 9 numeric digits can be used. After completing the above validations, the user will be successfully signed up and will be redirected to the login part.

3) QR Code: -

After successful login and sign up part, the user will be redirected to generating QR code page. When the QR code is scanned we will be getting an unique OTP no. and also unique id. Here unique id is given to know that who is login in. One unique Id will be assigned with the users email id. The Unique id will be already assigned to the user during login but the OTP generated will be dynamic so it will get updated as user generates QR code. That is every time we generate a QR code we will be getting a unique OTP no. but the identity no. remains the same.

Fig. 3 Generated QR

4) SQL Database: -

a) OTP Master: -

OTP Master and User Master both are created in SQL Server Management Studio to maintain the databases of users that have registered and trying to login. This is done to differentiate between the authorized users and unauthorized users. In OTP Master we have created 3 columns for unique id, OTP created and Date when the OTP is created. When the user try to login a unique id is assigned to that user and they can generate QR code. Every time a User try to generate the QR code each time a dynamic OTP is generated so every single time the user does that it will get updated in our database of OTP Master with different OTP.

b) OTP User Master: -

In OTP User Master database of users that have registered is maintained which contains unique user id that is assigned only once during time of registration and username, email, password

and contact number.

B. Hardware

In figure no 4, you can see how the hardware is put together. The Raspberry Pi, which serves as a minicomputer, is used to collect hardware and introduce the proposed model. A VGI cable for the monitor's display, as well as HDMI cables for the keyboard, mouse, and webcam, are connected to the Raspberry Pi's ports. A 12V power supply is included.

Fig. 4 System Hardware

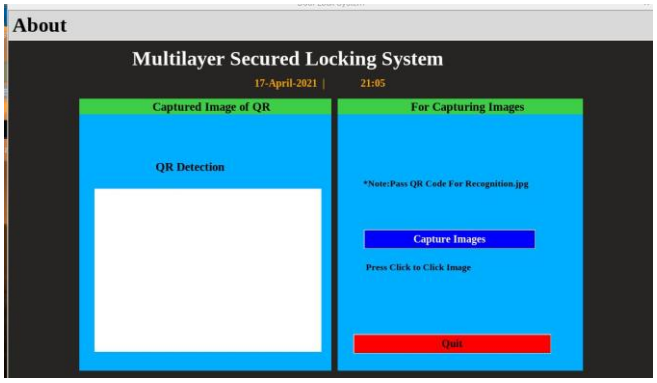

Fig. 5 QR Detection Frame-Window

The figure 5 shows the window that appears on the display for the user's convenience and interface. The window is divided into two frames, one for showing the captured QR image and the other for providing the command to capture the image as well as the option to leave.

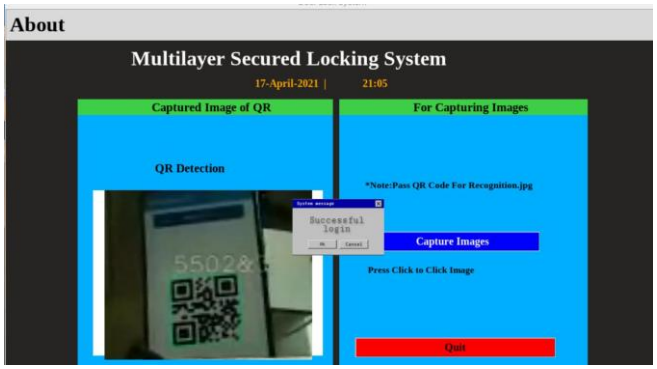

Fig. 6 Frame-Window after execution

VII. ALGORITHM

REALTIME QR CODE GENERATION & AUTHENTICATION

INPUT: Database (login ID (Li), Password (Ps)), OTP (Rand_number), Scrambling algorithm, change factor (Cf), Current Time (Ct), Time Set (Ts), change interval (Ci)
REQUIRE: Scanned QR code must match with the Database, then app will send acknowledgement to unlock.
PROCEDURE:

Login with ID and Password
QR code generated with OTP based on
QR = Li + Ps + $\frac{[Ct-Ts]}{Ci}$ * Cf
OTP = Rand_number
IF ([QR] + [OTP] = Database)
{
Return
{ "Successfully logged in"}
}
ELSE {
Return
{"Invalid entry"}
}
END

The algorithm for ***Realtime QR Code Generation & Authentication*** considers the namely input parameters: Database, that is (Login Id (Li) & Password (Ps)), OTP (Rand_number), Scrambling algorithm, change factor (Cf), Current Time (Ct), Time Set (Ts), change interval (Ci). The base requirement being that the scanned QR code must match with the one in the database, following which, the application will send an acknowledgement to unlock. The first step in the procedure is to login with a valid and registered ID and Password. After which the QR code is generated by the formula: $QR = Li + Ps + \frac{[Ct-Ts]}{Ci} * Cf$ and if-else loop helps in determining the steps to take if the QR and OTP are present in the database and similarly the step to take if they are not. The system returns a "Successfully logged in" message if the QR code and OTP are verified through the Database and a "Invalid entry" message if the QR code and OTP are not verified, respectively.

VIII. CONCLUSION

In In this paper, an idea was provided focusing on the security issues and considering the authentication and authorization of the user in question. A phone-controlled application also helps in guaranteeing the reliability and dependability. It was found that the proposed system was pocket-friendly and an easily implementable prototype. It also provides an understanding on how to manage home protection utilizing the encryption technique, i.e. QR code technology, keeping privacy in mind.

The model can be enhanced by the addition of either biometric scanner or RFID module, for well-defined security. Further expanding the opportunities in the home automation sector, the system can be utilized for higher authentication guaranteeing authorized access even widely.

REFERENCES

[1] [1] Nadaf, Raju, and Vasudha Bonal. "Smart Mirror using Raspberry Pi as a security and vigilance system." *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*. IEEE, 2019.

[2] Nagamma, N. N., M. V. Lakshmaiah, and T. Narmada. "Raspberry Pi based biometric authentication vehicle door locking system." *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*. IEEE, 2017.

[3] Devasena, C. Lakshmi. "Three-Factor Authentication for Fortified Login to Ensure Privacy Preservation and Improved Security." International Journal of Applied Engineering Research 13.10 (2018): 7576-7579.

[4] Kousalya, Sudha, et al. "IOT based smart security and smart home automation." *Int. J. Eng. Res. Technol.(IJERT)* 7.04 (2018): 2278-0181.

[5] Murugan, KH Shakthi, V. Jacintha, and S. Agnes Shifani. "Security system using raspberry Pi." *2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM)*. IEEE, 2017.

[6] Hussein, Naser Abbas, and Inas Al Mansoori. "Smart door system for home security using raspberry pi3." *2017 International Conference on Computer and Applications (ICCA)*. IEEE, 2017.

Bhargavi Kavalanekar is a student of Electronics and Communication Engineering and an Event head of IEEE UMIT, Usha Mittal Institute of technology, S.N.D.T Women's University, Santacruz (West), Mumbai, India.

Poorva Sankhe is a student of Electronics and Communication Engineering, Usha Mittal Institute of Technology, S.N.D.T Women's University, Santacruz (West), Mumbai, India**.**

Nikita Rathiwadekar is a student of Electronics and Communication Engineering, Usha Mittal Institute of Technology, S.N.D.T Women's University, Santacruz (West), Mumbai, India**.**

Umesh Mahind is Faculty at Usha Mittal Institute of Technology, S.N.D.T Women’s University. He is also pursuing PhD from Sardar Patel Institute of Technology, Mumbai. He has published 6 papers international conferences.