Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 2: 2025
ISSN : **1906-9685**

OTP Based Smart Wireless Locking System with Arduino for Home Security

SHAIK SAMEENA
DEP OF ECE
Anurag Engineering College
Kodada, India.
sameenashaik405@gmail.com

B.SWETHA
DEP OF ECE
Anurag Engineering College
Kodada, India.
bswetha.ece@anurag.ac.in

DARA SANDHYA
DEP OF ECE
Anurag Engineering College
Kodada, India.
sandhyadara08@gmail.com

S. TAGORE KHANNA
DEP OF ECE
Anurag Engineering College
Kodada, India.
tagoresiddamsetti@gmail.com

NANDIGAMA SRIRAM
DEP OF ECE
Anurag Engineering College
Kodada, India.
sriramnandigama08@gmail.com

Abstract: One novel approach to improving the safety and usability of conventional locking systems is the OTP-based smart Wireless Locking System that makes use of Arduino. An easy-to-use, secure lock system based on One-Time Password (OTP) authentication has been developed here by combining the power of wireless communication technologies with the capabilities of the Arduino microcontroller. Users must create a one-time password (OTP) using a specific mobile app in order to access the system. The one-time password (OTP) is safely sent to the command centre over a wireless communication protocol like Bluetooth or GSM. The specified wireless lock module is instructed to unlock by the central control unit after the validity of the one-time password (OTP) has been verified. A number of cutting-edge features have been included into the system to improve its usefulness and security. To start, the one-time password (OTP) increases security by reducing the likelihood of unauthorized access by using different passwords for each authentication attempt. Secure, dependable, and easy to use, the OTP-based smart Wireless Locking System utilising Arduino provides a contemporary answer to access control problems.

Keywords—*GSM, Keypad, Vibration sensor, Buzzer, Servo motor, Esp 32 Micro controller.*

I. INTRODUCTION

The protection of our possessions is of the utmost importance in today's technologically sophisticated society. Modern conveniences and security needs have outgrown the capabilities of old-fashioned mechanical locks. Consequently, cutting-edge options have surfaced, such as the smart wireless locking system that relies on an OTP (One-Time Password). An efficient and safe locking mechanism is created by harnessing the power of Arduino, a well-known open-source electronics platform, in the OTP based smart wireless locking system. By using a randomly generated, one-time password for every access attempt, this method does away with the need for actual keys. Users may remotely manage and monitor their locks using the smart locking system, which uses wireless communication technologies like Wi-Fi or Bluetooth. Connected to a trustworthy and secure one-time password (OTP) generating method, it creates a new password for every login attempt, making it very safe. Users are able to run the system with ease by entering the generated OTP using a specialized control panel or a smart phone application. After the Arduino checks the OTP, it locks or unlocks the device as needed. Notifications in real-time, access records, and the option to allow authorised users temporary or time-limited access are just a few of the extra features offered by the smart wireless locking system.

II.RELATEDWORK

Not a single system is appropriate for all sorts of applications, according to Pradnya R. Nehete, J. P. Chaudhari, and S. R. Pachpande [1], who have developed door lock systems based on biometric techniques and password-based systems. Both technology and methods of robbery are evolving at a rapid pace. The next step, therefore, is to design a novel, intelligent, and impenetrable method for use in research. Smart-Lock-System will pave the way for a plethora of advancements in the global realm of lock systems, according to Mr. Patil Bhushan, Mr. Mahajan Vishal, and Mr. Pawar Mayur [2]. A giant leap ahead in the pursuit of a better future lock system is assured by its minimal complexity, extensive application possibilities, simplicity of installation and usage, and high feasibilities. Considering one of the most important parts of the innovation, security is essential if any of the foregoing is to be believed or even attempted. The three modules, the keypad, the Bluetooth, and the gsm module, are able to control the servo motor, allowing S. Umbarkar, G. Rajput, S. Halder, P. Harname, and S. Mendgudle [3] to open and shut the door lock. When a user repeatedly enters the erroneous password three times in a row, the digital door lock system will send a message to the user's GSM mobile phone and activate a security buzzer. There have been analyses and surveys of various door lock systems conducted by Aishwarya I P [4]. The survey's findings provide light on the methods' relative merits and their potential uses in various contexts. Bypassing or defeating security measures is becoming more complex as technology progresses. Either by integrating existing security measures

or by introducing a new method that addresses the many shortcomings of the current system, a sophisticated door-lock security system has to be planned and built. An overview of the fundamentals of controlling a door automation security system using an OTP has been provided by Snehalata Raut, [5]. Additionally, it offers top-notch security and is user-friendly for Android phone users. The Android platform, which is open-source and free, is the foundation of this project. Therefore, the implementation rate is affordable and fair for both individuals and structures.

III.EXISTING METHOD

If smart locks aren't updated often, they may be easily tampered with. They are vulnerable to hacking since they are electronic devices, and IT professionals may use cell phones to generate bogus access codes. A brief loss of power in the control unit or an issue with the identification device [6-8]. Human mistake makes key loss a real possibility; carrying about a lot of keys makes them easy targets for thieves; and forgetting to shut the lock may lead to problems in situations when the lock won't close on its own.

IV.PROBLEM STATEMENT

If smart locks aren't updated often, they may be easily tampered with. They are vulnerable to hacking since they are electronic devices, and IT professionals may use cell phones to generate bogus access codes. A brief loss of power in the control unit or an issue with the identification device. People make mistakes all the time, which increases the likelihood of losing the key. Having a lot of keys makes them easy targets for thieves. Forgetting to close the lock is another common problem; mechanical locks don't rely on electromechanical systems to close themselves.

V.PROPOSED METHOD

An innovative and safe method of guarding a combined home security system is using an OTP (One-Time Password) Lock. In comparison to systems that rely on static passwords, this one-time password updates at regular intervals (often with each use), substantially increasing security. Because it incorporates the Arduino Uno, it's a flexible and inexpensive option for a lock like this.

Initiated in the code, the manual key sensor will send a One-Time Password (OTP) to a mobile phone via the Global System for Mobile (GSM). As soon as the OTP is received, the solenoid lock will open. The entire process will be displayed on an I2C LCD and controlled by an Arduino UNO master board.

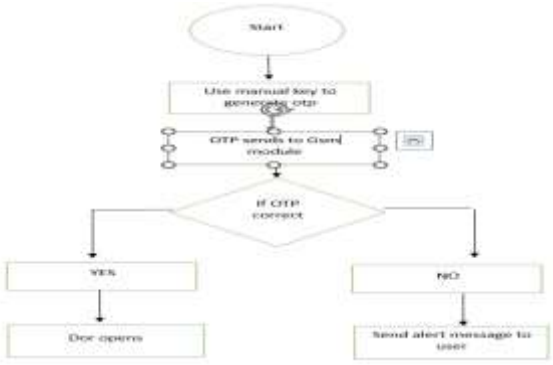

FIG1 PROPOSED FLOW CHART

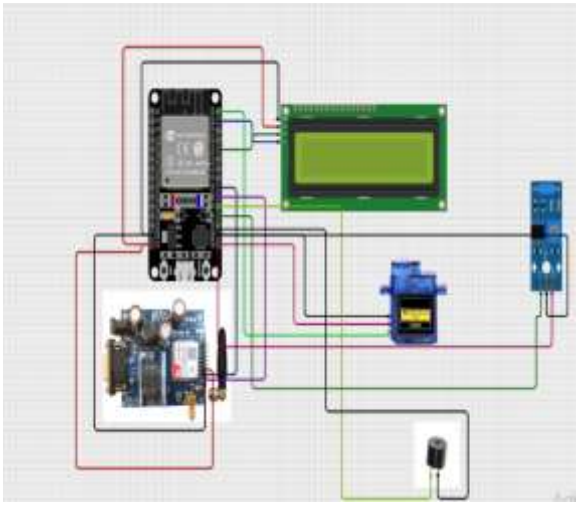

FIG 2 SCHEMATIC DIAGRAM

VI. RESULT

To access the system, the user is prompted to provide a valid one-time password (OTP). An app on a mobile device will produce the one-time password. Through Bluetooth, the Arduino board may receive the one-time password (OTP) sent by a mobile device. The Arduino board will check the received one-time password (OTP) against a database of legitimate OTPs or a pre-shared secret. The system will open the door or activate the electronic lock mechanism if the one-time password matches.

In order to prevent unauthorised persons from quickly accessing the OTPs, the system stores them securely. It is possible to increase safety by using methods like hashing or encryption. Both successful and failed attempts at access are recorded by the system. Both monitoring and auditing may benefit from this record. Adding, editing, or removing users and their associated OTPs is a function of this system. This is accomplished by the use of a specialised smartphone app. The quality of implementation, security measures, and software and hardware dependability will determine the general efficacy of the OTP-based smart wirelessly locking system. To make sure the system works and is reliable, it has to be tested and validated extensively.

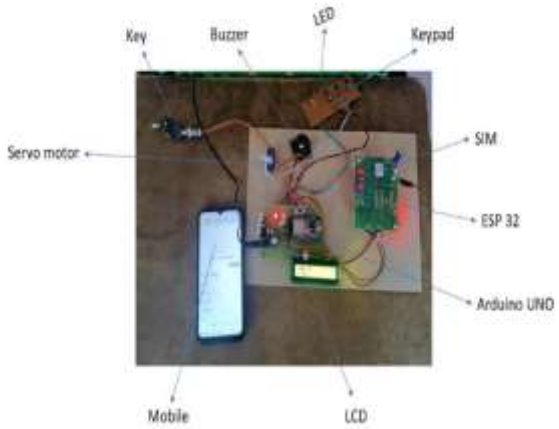

FIG 3 HARDWARE SETUP

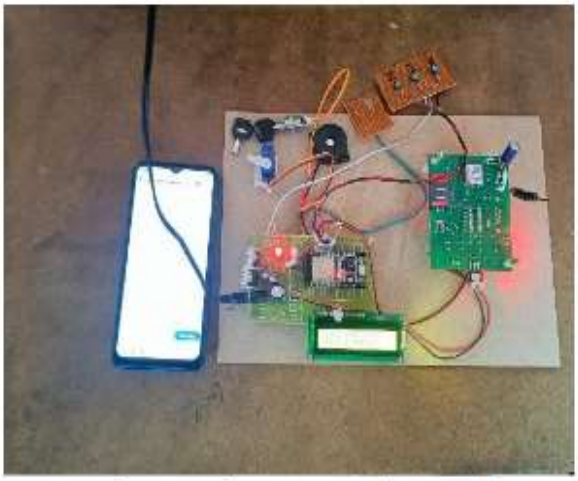

FIG 4 RECEIVED DATA TO CONCERNED SIM

FIG 5 DISPLAYING THE PHONE NUMBER IN LCD SCREEN

FIG 6 OTP GENERATED

If enter the correct mobile number, the OTP is generated, and it is exposing in the LCD display for opening the door.

FIG 7 ENTER OTP

FIG 8 IF OTP IS WRONG

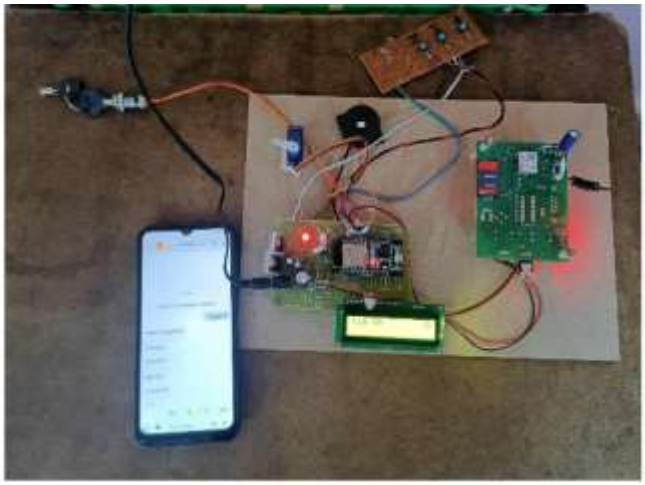

FIG 9 WHEN THE LOCK IS BREAKING, THE VIBRATE SENSOR IS ON THROUGH LED

From figure 4 to figure 9 exposes how registered sim will get notification of mobile number to generate OTP for secure home automation for avoiding thefting.

If we enter wrong number like not registered mobile number immediately sms will send to vibrator sensor to protect our home to alerting concern system.

VII. CONCLUSION

We frequently failed to bring the house key. Or occasionally, the door latch accidentally closes when we leave our house. It is really challenging to enter the residence in these situations. In addition to being safer, this paper will facilitate keyless entry. By utilizing Bluetooth in its place of GSM, which charges for tune-up, this concept will reduce overall costs. Because of their affordability and ease of use, smart door locks are among the most widely used digital consumer gadgets. Actually, it takes the place of a lot of ordinary locks. Since the Android platform is entirely based on free, open-source software, the implementation rate is likewise low and simple to install anywhere. This paper is sufficient to offer security as long as the password is kept private. Its primary benefit is the ability to access a door lock with an Android device, encrypting the password and sending a notification to the homeowner's mobile device each time the door opens. As a result, the proposed system can be completed faster than with other methods that were previously used.

VIII. FUTURE SCOPE

In addition to being ready for PIR proposition detectors, night visualization features, wide-angle cameras, and both side audio for distant communication, smart locks may soon incorporate smart camera technologies. There are countless chances for smart locks to develop into a comprehensive security tool. In future smart locking system is also integrated to AI for better performance.

REFERENCES

[1] Pradnya R. Nehete, J. P. Chaudhari,S. R. Pachpande Door lock security systems

[2] Mr. Patil Bhushan, Mr. Mahajan Vishal, Mr. Pawar Mayur Automatic door lock system

[3] S. Umbarkar, G. Rajput, S. Halder, P. Harname and S. Mendgudle Automatic door lock system

[4] Aishwarya I P A survey on smart door lock security methodologies

[5] Snehalata Raut, Dimple Chapke, Akash Sontakke , Nayan Pounikar, Prof. Neha Israni Door automation security system using OTP.

[6] Amanpreet Singh, Adarsh Sachan, Kashish Gupta, Gautam Kapoor, Harsh Kumar Singh, Ananya Singh IOT Based Smart lock

[7] Deeksha P, Mangala Gowri M K, Sateesh R , Yashawini M , Ashika V B OTP Based locking system using IOT

[8] Pradip Tilala, Anil K. Roy and Manik Lal Das Home access control through a smart digital locking-unlocking system