OTP BASED LOCKING SYSTEM

[1]Sowmya K S , [2]Preksha S A, [3]Nizamulla Khan, [4]Nihal T N
[1]*Assistant Professor*, [2,3,4]*UG Scholar Department of Information Science and Engineering,*
BMS College Of Engineering, Bangalore
Email: sowmyaks.ise@bmsce.ac.in , prekshasa.is19@bmsce.ac.in , nizamulla.is19@bmsce.ac.in , nihaltn.is19@bmsce.ac.in

Abstract: **This project proposes an OTP-based locker operation system which provides secure access to lockers using one-time passwords (OTP). The system is designed to enhance the security of locker access by ensuring that only authorized personnel can access the lockers. It also eliminates the need for physical keys and provides a more efficient way of managing locker access. This project is expected to provide a secure, efficient, and cost-effective locker access system. The main aim of the project is to provide a system wherein a person can access the locker only with the help of a valid OTP and the locker stays open only for a specified time. The user will be given a unique OTP which will be used to open the locker. The system will include an authentication process to verify the user's OTP and then unlock the locker. The system will provide an efficient and secure way of locker operation. Once the user enters the wrong OTP for a specified number of times then the locker will be disabled for a certain period. Every movement of the system will be conveyed to the main user. This project could be used for the safe and efficient delivery purpose of any commodity whenever no one is physically available to collect the commodity.**

Keywords: Arduino, One-time password (OTP), Security, Commodity delivery, Locker operation, Cost-effective, Usage records, Authentication

I. INTRODUCTION

In recent years, the need for secure and efficient access control systems has become increasingly important. One of the most common applications of access control systems is in the management of lockers. Traditional locker systems rely on physical keys, which can be lost, stolen, or duplicated, compromising the security of the lockers. To address this issue, this paper proposes a One Time Password (OTP) based locker operation system.

The OTP-based locker operation system provides secure access to lockers by using unique one-time passwords generated for each user. The system eliminates the need for physical keys and provides a more efficient way of managing locker access. The main aim of the project is to provide a system where a person can access the locker only with a valid OTP and the locker stays open only for a specified time. The user will be given a unique OTP which will be used to open the locker. The system will include an authentication process to verify the user's OTP and then unlock the locker.

In this paper, we describe the design and implementation of the OTP-based locker operation system. We explain the algorithms, models, and methods used to authenticate users and manage locker access. The results of the study show that the proposed system provides a secure, efficient, and cost-effective solution for locker operation.

II. MOTIVATION OF THE RESEARCH

Getting a delivery when there is no one at home is always a hustle. Usually, the delivery is left at the doorstep which is not at all safer thing to be done. To eliminate this problem, a locker is fixed to the wall beside the house which is equipped with the programmed system which opens the lock only upon entering the right OTP. Recently, electronic key systems have become one of the most popular security systems installed in many residents and business areas. A key feature of such programs lies in the credibility with which authorized persons can obtain access to departments throughout the secure system with interactive communication.

The motivation for this topic can be seen in the following ways:

A. Security

One-time passwords provide a high level of security as the password can only be used once, reducing the risk of it being exploited by a malicious third party.

B. Convenience

A one-time password system can be easily integrated into various applications, such as online banking, e-commerce, or any other application that requires secure access.

C. Flexibility

One-time passwords can be generated and sent to the user's mobile device, making it a flexible solution for users who are always on the go

D. Prevent fraud

One-time passwords can help prevent fraud by verifying the identity of the user who is trying to access a locked resource, reducing the risk of someone posing as the rightful owner.

E. Compliance

One-time password-based locker operation may also be necessary to meet various compliance requirements, such as those related to data privacy and security regulations.

III. RELATED WORK

[1] OTP Based Locking System using IOT is a system that combines OTP (One Time Password) technology with Internet of Things (IoT) technology to offer secure access to a physical or digital area. This method can be used to manage entry to a physical entrance or gate as well as to manage access to a website or other digital place.

[2] A very secure method created to prevent unauthorized access to locker contents is the Locker Security System using Facial Recognition and One Time Password (OTP). To make sure that only authorized users can access the locker's contents, it combines facial recognition technology with one-time passwords (OTPs).

[3] Designing and implementing an OTP-based (One Time Password) IoT Digital Door-lock System and Applications is the goal of this project. This system, which uses Internet of Things (IoT) technology to protect access to personnel and assets, is safe, practical, and automated.

[4] The Symbolic-OTP Based Security System for Domestic Use is a security system that improves user data and personal information security by combining symbolic and one-time passwords (OTP). A group of experts from the University of Science and Technology in South Korea created the system.

[5] A more secure method of securing doors is offered by the Iot Based Smart Door Lock System, a relatively new piece of technology. It offers a safe and practical solution to safeguard doors by combining Bluetooth and internet of things (IoT) technology. The system enables remote door lock control from any device. The system also comes with an easy-to-use mobile app that enables users to manage door locks, create access schedules, and get alerts when doors are opened.

[6] Design a user interface for the system that allows users to enter a one-time password (OTP) and select a locking action (e.g. lock, unlock, etc.). Design a secure communication protocol between the OTP system and the locking system. Determine the methods for the OTP system to verify the identity of the user. Create a database for storing user information, including passwords, lock status, and other relevant data. Design a system for securely storing and managing OTPs. Develop algorithms for generating and validating OTPs. Implement the OTP system's secure communication protocol with the locking system. Create a database to keep track of user data and OTPs.Create formulas for creating and verifying OTPs.Test the prototype using dummy data to make sure it performs as intended. Upload the prototype to a cloud hosting site so that it may be tested and assessed further.

[7] IOT's groundbreaking SMS-Controlled Smart Home System allows users to operate their home appliances from anywhere by sending a short text message. Users can use their smartphones or tablets to remotely operate current home automation systems and appliances thanks to the system's ability to integrate with them. The system is run by a central hub that communicates with the user's current home automation system and issues instructions to the associated devices. The user can then utilise text messages to send commands to the hub, which are then transmitted to the linked devices. The system also comes with an app that can be used to schedule automated operations as well as monitor and control the linked devices.

[8] This study compares various DC servo motor position control strategies with position feedback using Arduino. The proportional-integral-derivative (PID), fuzzy logic, and sliding mode control approaches are taken into consideration in this work. Position accuracy, settling time, and overshoot are used to assess how well each method performs. In terms of position accuracy and settling time, the results indicate that PID control performs best, while sliding mode and fuzzy logic control have the lowest overshoot. The PID control has the lowest overshoot, whereas the fuzzy logic control performs the best in terms of overshoot. The findings of this study show that PID control is the most effective technique for

[9] The microcontroller board known as Arduino is used to manage electrical appliances. It is programmed using an Arduino-compatible computer. The Arduino board can be wirelessly or via a USB cable connected to a computer. The board interprets signals sent to it from the user's computer and carries out the requested actions. Lights, motors, sensors, and other devices can all be managed by it.

[10] A wireless technology called a GSM-based home appliance control system can be used to control household appliances from a distance. It transmits and receives signals from the user's mobile phone using GSM (Global System for Mobile communication) technology. Through an SMS or phone call, this system may be used to manage and keep an eye on the appliances from any location. It can be used to turn appliances on and off, check on their status, and even create an automated timer for turning them on and off. The technology is affordable, simple to install, and efficient. It can

also be used to track energy use and aid in energy conservation.

[11] The proposed IOT based low-cost smart locker security system is a secure and automated system which is designed to protect the belongings and valuables of individuals in locker rooms. The system is designed using the concept of Internet of Things (IoT) which is a technology that helps to connect physical devices over the internet.

[12] Propose a keyless smart home security system using Bluetooth for automated door locks, combining Android as signal sender, Bluetooth comm. module, Arduino microcontroller as CPU, and servo motor/LEDs for output.

[13] The vital zones are meant to have the highest level of protection possible thanks to this safe door lock mechanism. A keypad, a computerized lock, and a remote control are all part of it. The administrator-set access code must be entered using the keypad. The keypad and remote control are both wired to the digital lock. The door can be remotely unlocked or locked using the remote control. These parts are all linked to a central control unit that is part of a network. Only authorized users will be able to access this network thanks to its strong security mechanisms. Other security systems, such CCTV cameras, biometric scanners, and motion sensors, can be incorporated with the system.

[14] An IoT-based smart locker system called LockerSwarm gives businesses and organizations access sharing and safe storage options. The management of lockers and other safe storage places will be automated by the system. It also makes it simpler for users to share their lockers with other users and gain access to them.

[15] A detailed survey on “Various Door Lock Access Control Mechanisms” and comparison between them

IV. PROPOSED SYSTEM

The system includes the following components:

A. Arduino Uno

Arduino Uno is a microcontroller board based on the ATmega328P microcontroller. The Arduino Uno has 14 digital input/output pins, 6 analog inputs, a 16 MHz quartz crystal, a USB connection, and an integrated power supply. The board can be programmed using the Arduino Integrated Development Environment (IDE) and supports C/C++ programming languages. The Arduino Uno is compatible with a wide range of sensors, actuators, and other components, which makes it an ideal platform for a variety of projects.

B. 4x4 numerical keypad

A 4x4 numerical keypad is a type of input device that consists of 16 buttons arranged in a 4x4 matrix. The buttons are typically labeled with the numbers 0 to 9, as well as with other symbols such as *, #, A, B, C and D . The 4x4 numerical keypad is commonly used for numerical data entry and control applications, such as for entering PIN numbers, accessing secure systems, or controlling electronic devices. The 4x4 numerical keypad works by using a matrix scanning technique to detect which button is pressed. When a button is pressed, the corresponding row and column lines are connected, which allows the microcontroller to detect the button press. The microcontroller then sends a signal to the system to process the input.

C. I2C 1602 module

A I2C 1602 module is a type of LCD (Liquid Crystal Display) module that is commonly used for displaying text and characters in a variety of applications. The 1602 in the name refers to the number of characters that the module can display, which is 16 characters per line and 2 lines in total. The I2C in the name stands for Inter-Integrated Circuit, which is a type of communication protocol used to transfer data between the module and a microcontroller or other type of device. The I2C 1602 module typically includes an LCD display and a control circuit that is capable of communicating with other devices using the I2C protocol. The module can be easily connected to a microcontroller, such as the Arduino, by using only a few pins, allowing for easy integration into a wide range of projects.

D. LCD

LCD stands for Liquid Crystal Display, which is a type of flat panel display technology that is commonly used in a variety of electronic devices. An LCD display works by using a liquid crystal material that is sandwiched between two transparent electrodes. When an electric field is applied to the liquid crystal material, it changes its orientation and allows or blocks light from passing through, creating an image. Behind the liquid crystal layer, there is a backlight that provides illumination, which allows the user to see the image.

E. Relay

A relay is an electrically-operated switch that opens or closes a circuit by means of an electromagnet. The term "relay" refers to the switching mechanism that is activated by an electrical signal, which in turn opens or closes the contacts of the switch. Relays are commonly used in a variety of electrical and electronic applications as a means of controlling electrical circuits without the need for direct human intervention.

F. SIM800L

It is a compact, low-power and cost-effective cellular communication module that supports GSM/GPRS networks. It is designed to provide a simple and efficient way of adding wireless communication capabilities to a wide range of devices, including

microcontrollers, single-board computers, and embedded systems. The SIM800L module is equipped with a powerful 32-bit processor, a high-performance GSM/GPRS engine, and a built-in TCP/IP stack that supports a wide range of communication protocols. It supports voice and data communication, as well as SMS and Internet connectivity. This makes it ideal for a variety of applications, including remote control, telemetry, machine-to-machine (M2M) communication, and the Internet of Things (IoT). The module is compatible with a wide range of microcontrollers, such as the Arduino and Raspberry Pi, and it can be easily integrated into existing projects by connecting it to the microcontroller through its serial interface. The module also supports a wide range of power sources, including USB and battery, making it ideal for portable applications. Overall, the SIM800L module is a powerful and versatile cellular communication module that provides a simple and efficient way of adding wireless communication capabilities to a wide range of applications.

G. Solenoid Lock

A solenoid lock is a type of lock that uses an electromagnetic coil, known as a solenoid, to control the movement of a latch or lock. When the solenoid is energized, it creates a magnetic field that pulls a plunger or armature towards it, which in turn actuates the lock mechanism. This mechanism can be used to lock or unlock doors, cabinets, safes, or other types of enclosures that require secure access control. Solenoid locks offer several advantages over traditional mechanical locks, including improved reliability, faster lock/unlock times, and the ability to remotely control the lock. They are often used in a variety of applications, including access control systems for buildings, security systems for safes and vaults, and locking mechanisms for electrical cabinets and enclosures. Solenoid locks come in different configurations, including those with a single solenoid, double solenoid, or multiple solenoids. The number of solenoids used in the lock will depend on the specific requirements of the application, such as the strength of the magnetic field needed to actuate the lock, and the desired level of security. Overall, solenoid locks are a versatile and convenient locking solution for a wide range of applications. They offer improved reliability, faster lock/unlock times, and the ability to remotely control the lock.

H. IR Sensor:

An IR sensor, or Infrared sensor, is a device that detects infrared radiation and converts it into an electrical signal. Infrared radiation is a type of electromagnetic radiation with a wavelength longer than visible light, but shorter than microwave radiation. IR sensors are commonly used in a wide range of applications, including remote controls, security systems, obstacle detection and avoidance systems, and temperature sensing. IR sensors typically consist of an IR-sensitive photodiode or phototransistor that detects the incoming IR radiation and converts it into an electrical signal. This electrical signal is then processed by the sensor's electronics to provide an output that indicates the presence or absence of IR radiation. Some IR sensors are designed to detect only the presence of IR radiation, while others are capable of measuring the intensity of the radiation and converting it into a corresponding electrical signal. IR sensors are used in many consumer electronics products, such as televisions, air conditioners, and remote controls, to detect user inputs. They are also used in industrial and commercial applications, such as thermal imaging cameras, and in robotics and autonomous systems, such as obstacle detection and avoidance systems.

I. DC-DC buck converter

A DC-DC buck converter is an electronic power converter that is used to convert a higher voltage DC (direct current) power source into a lower voltage DC power source. It works by controlling the amount of power that is transferred from the input to the output by changing the duty cycle of a switch. The name "buck converter" comes from the fact that it reduces, or "bucks," the input voltage. The converter consists of a switch, an inductor, a capacitor, and a control circuit. The switch is typically a metal-oxide-semiconductor field-effect transistor (MOSFET) that is used to regulate the amount of current flowing through the inductor. The operation of a DC-DC buck converter is based on the principle of energy storage in an inductor. When the switch is closed, current flows through the inductor and the energy stored in the magnetic field of the inductor is transferred to the output. When the switch is opened, the energy stored in the magnetic field of the inductor is transferred back to the output and the voltage across the inductor collapses. This collapsing voltage, combined with the input voltage, results in a higher voltage at the output than would otherwise be possible.

Here initially when the IR sensor senses the waiving from the user, Arduino with the use of SIM800L module generates a random one time password of length 4 digits and is sent to the owner of the locker and also saves the generated password into the Arduino’s RAM. When OTP is entered into the 4x4 numerical keypad, the entered digits are displayed in the LCD with the help of I2C 1602 module. This module helps in reduction of the number of pins used and converts serial data

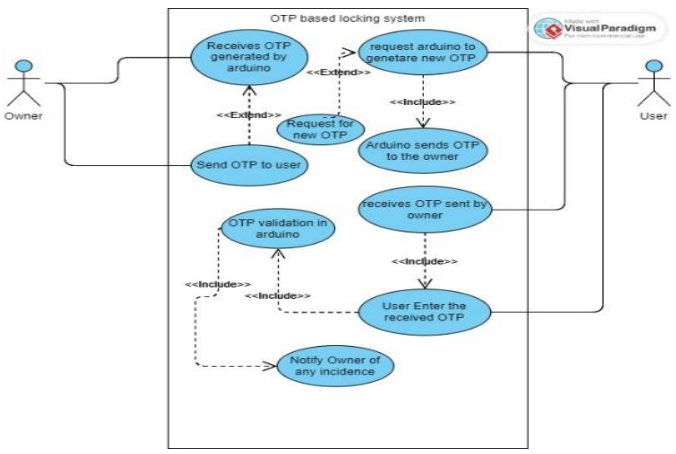

FIG. 1 USE CASE DIAGRAM

into parallel data. Whenever 4 digits are entered to the system, the Arduino Uno authenticates the entered password with the password stored in the Arduino's RAM. When the authentication is successful, the solenoid lock opens else the lock remains closed. If the lock is opened, the Arduino is programmed in such a way that the locker closes automatically after a certain time without users intervention.

V. METHODOLOGY

The locker system requires the user of the locker to wave at the IR sensor to trigger the locker system. This action will generate the One Time Password in the system and send it to the owner of the locker and also stores the one time password in the RAM of the Arduino board. Once the owner gets the One Time Password and if he believes the user to be authentic, he sends the One Time Password to the user. The user must enter the One Time Password provided by the owner on to the 4x4 numerical keypad provided and can observe whatever is being entered through the LCD display. Once the user enters the 4 digit completely, the system verifies the password entered with the password stored in the Arduino's RAM. This is done for password authentication and verification. The solenoid lock opens only if the entered password is valid else remains closed. If the locker is opened, the microcontroller is programmed in such a way that the lock closes automatically without the intervention of the user or the owner. The system automatically locks after a certain period of time. Whatsoever actions are performed on the system, all the activities are notified to the owner of the locker. Be it the locker successfully opening after authentication, the locker not opening on entering wrong password, multiple entries of wrong password to gain access to the locker or request for a new password, all such actions are notified to the owner.

A. Algorithm

This project uses the random password generation in order to operate and the steps are as follows:

- To unlock the lock, user have to wave at the IR sensor.
- And then the random number generation method called, and it creates series of random number.
- The generated number sent to the registered mobile number in the programming part.
- Then the number is stored in the microcontroller
- After that user must enter the number which he has received.
- Then the entered the number and the stored number to be compare.
- If both are same or matched the locker will be open
- Otherwise, it remains locked.
- The locked door will close automatically close after a given time.
- All the events are conveyed to the owner of the locker.

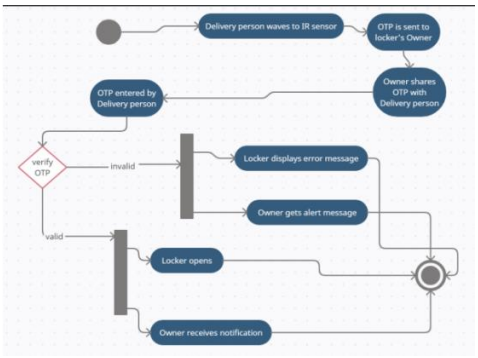

FIG. 2 ACTIVITY DIAGRAM

VI. CONCLUSION

In conclusion, the One-Time Password (OTP) based locker system is a cutting-edge technology that has revolutionized the way organizations manage access to their lockers. This system provides a secure, convenient and cost-effective solution for locker management. One of the key benefits of this system is its high level of security. By generating a unique OTP for each transaction, the system ensures that only authorized users can access the lockers, reducing the risk of theft or unauthorized access. This added layer of security is especially important in industries where sensitive and confidential information is stored in lockers. Another advantage of the OTP-based locker system is its ease of use. Users simply need to enter the OTP into the locker system, and the locker will automatically unlock. This eliminates the need for users to remember multiple passwords or carry physical keys, making the system highly user-friendly. The system can also be easily integrated with existing security systems, such as biometric authentication or smart cards, making it a flexible and scalable solution. This makes it an ideal choice for organizations that need to manage a large number of lockers, as the system can be easily customized to meet their specific needs. Finally, the OTP-based locker system is a cost-effective solution for organizations. By reducing the need for physical keys, which can easily be lost or stolen, the system eliminates the need for frequent replacements and saves organizations money in the long run. In summary, the OTP-based locker system is a reliable and secure solution that provides organizations with peace of mind, knowing that their valuable assets are protected. By implementing this system, organizations can ensure that their lockers are secure and their sensitive information is protected.

VII. REFERENCE

[1] Deeksha P, MangalaGowri M K ,Sateesh R ,Yashaswini M,Ashika V B "*OTP Based Locking System using IOT*",2021

[2] N. Anusha, A. Darshan Sai and B. Srikar , "*Locker Security System Using Facial Recognition and One Time Password (OTP)*",2017

[3] Joongjin Kook , *"Design and Implementation of a OTP-based IoT Digital Door-lock System and Applications*",2018

[4] Kantilal P Rane, "*Symbolic-OTP Based Security System for, Domestic Use*" ,2020

[5] G. Sowmya, G. Divya Jyothi, N Shirisha, K Navya, B Padmaja, "*Iot Based Smart Door Lock System*" ,2018.

[6] Sreekanth S, Sandeep M, Santhosh N, Devaraja M V and Kalaiah J B , "*Design and prototype development of OTP based advanced digital locking system*" , Volume:03/Issue:07/July-2021.

[7] S.Amudha Mary, T.S.ShinyAngel and N. Snehalatha , "*SMS Controlled Smart Home System In IOT*", Vol.8, No.1 Nov 2016.

[8] Amirul Syafiq Sadun, Jamaludin Jalani and Jumadi Abdul Sukor, "*A comparative study on the position control method of dc servo motor with position feedback by using Arduino*",vol.11, no.18, September 2016.

[9] Yusuf Abdullahi Badamasi, "*The Working Principle Of An Arduino*", 2014 IEEE.

[10] Mrs Khin Ei Ei Khine, Mr Nay Soe Shwe and Mr Aung Myo Naing, "*GSM Based Home Appliance Control System*", Volume 3 Issue 5, August 2019.

[11] L. Nagarajan and A. Arthi, "*IOT Based Low Cost Smart Locker Security System*", Volume 3, Issue 6 ISSN: 2454-132X.

[12] Amrita Dewani ,Sania Bhatti,Pirah Menon,Veena Kumar ,Anum Arain and Ayaz Jiskani, "*Keyless Smart Home: An Application of Home Security and Automation*", ISSN: 0974- 6471,Vol 11, No.(2) 2018, Pg. 107-114.

[13] Meera Mathew and Divya R S , "*Super Secure Door Lock System For Critical Zones*", |20- 22 July 2017|.

[14] J. Sa-ngiampak, C. Hirankanokkul, Y. Sunthornyotin, J. Mingmongkolmitr, S. Thunprateep, N.Rojsrikul,T. Tantipiwatanaskul, K Techapichetvanich, A. Pongsawang, T. Prayoonkittikul,U.Wattanakulchart, N. Prompoon, C. Ratanamahatana and M. Pipattanasomporn , "*LockerSwarm: An IoT-based Smart Locker System with Access Sharing*", 5th IEEE ISC2 2019.

[15] Meera Mathew and Divya R S , "*Survey on Various Door Lock Access Control Mechanisms*", 2017 International Conference on circuits Power and Computing Technologies [ICCPCT].