Journal of IoT in Social, Mobile, Analytics, and Cloud (ISSN: 2582-1369)
www.irojournals.com/iroismac/

An IoT-based Smart Security Locker System with OTP Verification

Biplov Paneru[1], Krishna Bikram Shah[2], Bishwash Paneru[3]

[1]Department of Electronics and Communication Engineering, Nepal Engineering College, Pokhara University, Bhaktapur, Nepal

[2]Department of Computer Science and Engineering, Nepal Engineering College, Pokhara University, Bhaktapur, Nepal

[3]Department of Chemical Science and Engineering, IOE Pulchowk Campus, Tribhuvan University, Lalitpur, Nepal

E-mail: [1]biplov001@gmail.com, [2]krishnabs@nec.edu.np, [3]rampaneru420@gmail.com

Abstract

Due to frequent movements and hangouts between classrooms and office buildings, students' personal items/expensive gadgets can get lost, misplaced and stolen, this has become a common issue that people across the campus and offices have been frustratingly dealing with. Keeping this in mind, this research work aims to implement a cost-effective "Password-Based Locker Security System" to protect the personal assets of students and staff, like laptops, gadgets, keys, and personal documents. The study presents a prototype security locker that utilizes Arduino UNO connected with a Wi-Fi module, which controls the complete processes like taking a password from the keypad module, comparing passwords, driving the buzzer, triggering the relay, and sending status to the LCD and connecting to the Internet of Things (IoT). The system is based on IoT technology using the Blynk IoT platform, which sends a notification alert to the connected device in case of security breaches. One Time Password (OTP) verification can be done to reset the password after three wrong password inputs. The proposed system is portable, durable, and installable in specific places.

Keywords: Password-Based Locker Security System, Campus Security, Personal Asset Protection, IoT-enabled Security System, Arduino-based Security.

DOI: https://doi.org/10.36548/jismac.2023.3.001
Received: 05.06.2023, received in revised form: 02.07.2023, accepted: 14.07.2023, published: 27.07.2023

1. Introduction

In this era of rapid technological advancement, the electronic security system has become one of the cheapest preventative measures to protect business and personal assets such as money, property and even intellectual property that are under non-disclosure agreements [1]. Security is now more important than ever. The risk of misplacing or losing your belongings or getting your assets stolen/robbed is just as rampant in an educational institution as in big companies and businesses [2]. With the massive influx of storage and security systems being used by homeowners, business owners, banks, hospitals, and corporations alike, it is only pertinent that a similar approach be introduced on the premises of educational institutions as well.

These security and storage solutions are exceedingly costly despite their necessity [3]. In this sense, the research aims to offer students a secure and cost-effective storage system. The research intends to contribute by providing students with a cost-effective storage and security system. A college is continually active, with many students moving from one classroom to another and congregating outside classes. It is only sometimes practicable for students to bring their expensive and essential equipment to campus due to the risk of losing, breaking, or being stolen. Numerous students have misplaced little goods such as keys, watches, etc. Students have been coping with this persistent and frustrating problem for years. This research aims to construct a "Password-Based Storage and Security System" tailored to students' needs.

This security system is designed to be implemented on individual floors of a college building and in individual classrooms if possible. The design will consist of a locker to fit the students' gadgets/personal belongings to act as storage. The locker will have a 16-character matrix keypad to enter the password provided to the individual concerned. It will give a person three tries before triggering the signal to ring the buzzer that will alert the individuals nearby of possible malicious intent. This way, the students can be reassured and at ease knowing their personal belongings are safe even in their absence in the classroom/building.

This research aims to design and develop a password-based locker system with the following objectives.

- To develop a password-based locking system based on the Internet of Things
- To develop an OTP-based password reset system
- To make a portable and advanced security locker.

2. Literature Review

The rapid adoption of security systems in numerous facets of modern life has become indispensable in recent years. Individuals are increasingly concerned about their valuables' safety, whether stored in enterprises, organizations, or bank lockers. However, conventional security measures, such as safe lockers that require a PIN, have been shown to be susceptible to unauthorized access. To address this issue, researchers have proposed novel solutions that integrate face recognition, biometric technologies, and the Internet of Things (IoT) to bolster the security of safe boxes and door locks.

The main purpose is to provide security in all public places, such as homes and public places, and all system information is stored in the cloud. After entering the required code, the microcontroller feeds the coil to the servo motor, helping to lock or unlock the door as needed. M. S. Zaghloul et al. 2014 [4] describe the research, which aims to create and use new computing technologies to create shared security and make them suitable for ordinary citizens and large organizations.

Some additional functions, such as adding new users and changing old passwords, can be set on the keyboard as usual. The screen adopts the LCD model. These machines rarely have instruction manuals. Therefore, flexibility and reliability are high. It controls them using GSM technology and allows users to control the operation remotely, as described by J. F. Li et al. 2015 [5]. The paper also shows that building security is cost-effective for better use.

the use of pre written password to open the door increases the security level to prevent unauthorized access by intruders. The system proposed by M. A. Hossain et al. 2016 allows users to change or reset both passwords if they forget them easily [6]. This password-based automatic locking system will provide users with a more secure locking system. First, the user's combination is compared to a pre-written password stored in the system memory. Users can test some connections before the system shuts down temporarily. If the user combination matches the password, the door will be unlocked. The same principle can be used to lock the door. The system will also allow users to reset their passwords if they wish.

In everyday life, cryptographic systems are important to ensure that everything or place is secure. The article by P. R. Nehete et al. 2016 [7] has used this to identify and create a safe path to a door that requires a password. A keypad is used to enter a code into the system, and if the code is entered correctly, the door is opened by a motor to rotate the door lock handle.

N. Anusha et al. 2017 [8] present a novel approach to enhance locker security by incorporating IoT, facial recognition, and OTP technology. When an individual wants to access the locker, a PIN is entered. The system captures the user's image and compares it with database records using Eigenface and PCA algorithms if valid. If the image matches, an OTP is generated and sent via SMS and email for added security. Transaction logs are sent to the registered number and email in cases of non-matching features, allowing owners to report intruders to the police promptly. This research aims to provide a comprehensive understanding of the proposed locker security system and its potential implications in overcoming current security challenges faced by locker systems.

Lokesh et al. 2017 [9] introduce a user-friendly, cost-effective IoT-based smart storage security system designed for both home and office use. The system aims to provide the general public with a secure method to protect their valuables, such as jewellery, money, and important documents, even when they are away from the locker's location. Utilizing an Arduino with a GSM module and incorporating a biometric scanner, the smart locker system sends prompt alerts to the owner's mobile device in case of security violations or unauthorized access attempts.

Kook 2019 [10] introduces an OTP-based IoT door-lock system designed to address the security concerns of single-family households, particularly those headed by single women. The system includes OTP password generation, remote lock control, image storage, and live streaming capabilities. In addition, a smartphone app provides enhanced security through real-time video surveillance, door lock control, and event logging.

Mohammed et al. 2019 [11] concentrate on designing and implementing an access-control system based on a combination of Password and Radio-Frequency Identification (RFID) technology. The system seeks to restrict locker access to only authenticated users. A passive RFID reader is used to read the ID number from the RFID tag, and a keypad is used to input a password. The locker will unlock if the ID number and the password are entered correctly. The primary objective of this study is to develop a robust, cost-effective, and error-reducing storage security system. This literature review aims to provide an overview of the proposed locker security system based on Password and RFID technology, emphasizing its potential implications for enhancing access control and ensuring secure storage. The research presents a novel strategy for resolving locker security issues by integrating two distinct yet complementary authentication mechanisms.

Setyadi et al. 2020 [12] discuss the limitations of conventional safe cases and propose a prototype with enhanced security is proposed. Face recognition and fingerprint technologies are utilized in conjunction with a two-way verification process and an incorporated Internet of Things (IoT) system. Notifications from Android apps make real-time monitoring possible. Under bright conditions, the face recognition system performs reliably, whereas fingerprint identification functions best on a flat surface. The system's distance and throughput values are optimistic in both line-of-sight and non-line-of-sight conditions.

Yulianto et al. 2022 [13], addresses the increasing concern over criminal acts such as robbery, especially in urban areas. To prevent theft attempts, safe-deposit lockers have been utilized to safeguard valuables. The research concentrates on implementing a secure security system that employs fingerprint technology and is connected to the internet via the Blynk application in order to increase security. The biometric sensor functions as the safe's access control, while the Arduino Uno microcontroller stores the command logic. In addition, a stepper motor serves as an actuator to open and close the safe, and the Esp8266 module connects the system components to the Blynk application via the internet network. Utilizing the Internet of Things (IoT) concept enables remote control and notification of residential access.

In conclusion, the above literature survey highlights the significance of instituting advanced security systems to protect personal belongings and valuable devices from theft and loss in dynamic environments such as educational institutions and offices. The examined research papers propose various solutions, including password-based locker systems, Internet of Things (IoT)-based smart storage security, face recognition, biometric technologies, and cryptographic methods. These cutting-edge methods address security concerns and provide real-time monitoring and notification alerts, enabling prompt responses to security breaches. These initiatives contribute to creating safer and more secure spaces for students, staff, and the general public by combining modern technologies with portable, cost-effective designs.

3. Proposed Work

The research presents a prototype security locker that utilizes Arduino UNO as a microcontroller. The Arduino UNO is an open-source microcontroller board based on the ATmega328P [14], which controls the complete processes like taking a password from the keypad module, comparing passwords, driving the buzzer, triggering the relay, and sending the status to the LCD. The door lock system uses a matrix keypad as the main input source since

the keyboard is directly connected to the microcontroller I/O pins without any communication interface. An I2C LCD display is a primary peripheral display where the user can see the input password or any essential information on the LCD display. The LCD uses the I2C communication protocol to receive its data. A solenoid lock is used as an actuator for the bolt in the door. Based on the input of the password, the lock is actuated. A sim 800L module is used to send OTP code to that particular sim module connected card, which unique number is defined in the program. The Esp8266 Wi-Fi module has been used to connect the Arduino to the IoT-based technology. And, for the wrong password, an OTP code message is sent to the user's mobile phone to reset the password using that OTP code. Powering the system is an off-the-shelf 2-ampere 12-volt power supply that can simultaneously power all the attached peripherals. A very lightweight & power-efficient buzzer is used for audible feedback.

First, the user combination will be compared to passwords previously recorded and kept in the system memory. Users are permitted several incorrect password attempts before the system is temporarily disabled. The door will unlock if the user combination and password match. Suppose the wrong combination is entered more than the specified number of times. In that case, the buzzer will emit an audible beeping sound signalling an emergency linked to an intrusion or a security breach.

3.1 Block Diagram of System

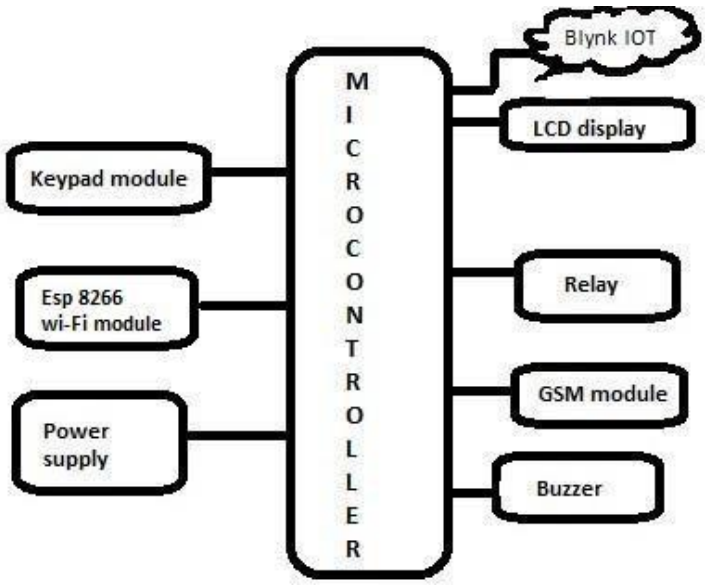

Figure 1. Block Diagram of the System

The brain of this proposed work is the microcontroller, the Arduino Uno board, and it is connected with the Esp8266 wi-fi module to connect the device to the internet and develop

an IoT-based system. The Arduino board is connected to an LCD, keypad, relay and buzzer. The relay is used to trigger the solenoid lock connected with the 12V supply and relay. The solenoid lock opens or closes the locker according to the entered password. A 16*2 LCD is required to display the message by Arduino; 16*2 means it has 16 columns and two rows. The buzzer rings if the password is entered wrong three times.

3.2 Working Principle of the System

1 Initialize the required libraries and variables:

1.1 Import the necessary libraries, such as Keypad, Blynk, GSM, and Wire.

1.2 Define variables to store the password, entered password, and the number of incorrect attempts.

2 Set up the keypad and Blynk:

2.1 Configure the keypad library to listen for button presses and assign it to a specific pin configuration.

2.2 Initialize and connect the Blynk library to the Blynk server using the appropriate authentication token.

2.3 Set up the Blynk virtual pins for notification purposes.

3 Set up the GSM module:

3.1 Configure the GSM module with the required parameters, such as baud rate, APN, PIN, etc.

3.2 Using the GSM module, set up a function to send an OTP message to a specified phone number.

4 Set up the buzzer:

4.1 Define the pin for the buzzer.

4.2 Implement a function to activate the buzzer for a specified duration.

5 Define functions for password verification and resetting:

5.1 Implement a function to verify the entered password against the stored password.

5.2 If the password is correct, grant access and reset the incorrect attempts counter.

5.3 If the password is incorrect, increment the incorrect attempts counter.

5.4 If the incorrect attempts counter reaches three, send an OTP message, activate the buzzer, and notify Blynk.

6 Implement the main loop:

6.1 Continuously listen for keypad input.

6.2 When a key is pressed, append it to the entered password.

6.3 Check if the entered password matches the stored password.

6.4 Based on the verification result, either grant access or perform the necessary actions for an incorrect password.

7 Implement the OTP verification and password reset function:

7.1 When an OTP is received, compare it with the entered OTP.

7.2 If they match, allow the user to reset the password.

7.3 Store the new password and reset the incorrect attempts counter.

8 Send Blynk notifications:

8.1 When the incorrect attempts counter reaches three, send a notification using Blynk to alert the user.

3.3 Flowchart of the System

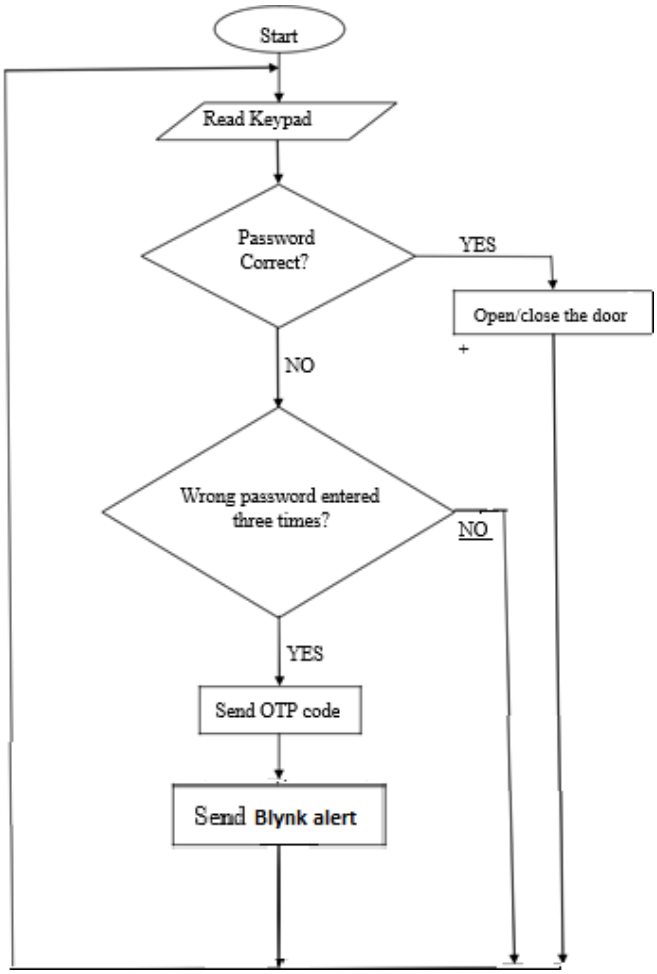

Figure 2. Flowchart of the System

As seen in Figure 2 above. The user is let to input the password, and if it becomes true as registered in the program, the system lets the relay or solenoid lock open and give access to the door. In case of a wrong password three times, the OTP message and notification of Blynk are sent during any sort of unauthorized access to the system. The user gets a message for OTP code sending requirement or not on-screen and if the user press one, the OTP gets sent to the user's phone, and the user gets prompted to reset part of the system when OTP is sent to the user's mobile phone. The Wi-Fi module connects the device to IoT, and the Blynk notification of unauthorized access is sent to the respective IoT-connected device using the Blynk platform.

In this research a 12V 2A AC-DC adapter is given to Arduino and a solenoid lock. This 12V is converted into 5V by a voltage regulator in the Arduino and given to peripheral devices through Arduino required for the operation. The Esp8266 wi-fi module has been connected to the Arduino UNO using standard serial communication, and a voltage divider circuit has been

employed for the purpose of the safety of the module. The SIM 800L is used to establish network communication for sending OTP messages.

The 4*4 matrix keypad is used, which is required to input passwords and manually lock our customized door locker. It consists of 16 keys, four in rows and four in columns. When the key is pressed, it establishes the connection between the corresponding rows and columns. It is also connected to Arduino.

3.4 Hardware and Software Used

Table 1. Security Locker System Hardware Components Implemented

Component	Function
Arduino Uno	Microcontroller board for overall processing
Esp8266 wifi module	Connecting to the Internet and building an IoT system
Relay	Actuating the solenoid lock
Solenoid Lock	Lock triggered by relay for door open/close.
Adapter	Adapting accurate voltage for the system
Sim800L module	Connecting to a GSM network for sending OTP message
Buzzer	Alert sound for unauthorized access to the system

Table 2. Security Locker System Software Components Implemented

Software	Functions
Arduino IDE	Programming of system
Blynk	IoT platform for getting notification alert
Proteus	Simulating the project virtually

4. Result and Discussion

Simulation of the proposed system consists of Arduino UNO, Buzzer, Keypad, Relay, and LCD, as shown in the diagram below. A lamp is used to determine if the system is working. The analogue digital pins of the microcontroller (Arduino) are connected to the respective pins of the keypad, buzzer, relay, LCD and virtual terminal. The simulation and pin configuration are as shown below:

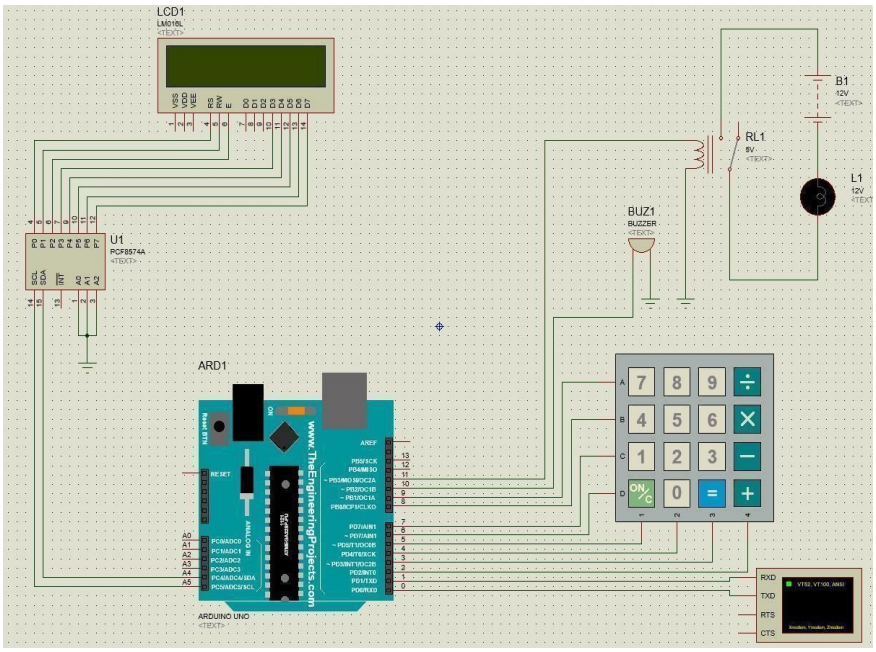

Figure 3. Simulation Circuit

This simulation uses a lamp instead of a solenoid lock to determine if the system works. When the required code is entered into the Arduino of the simulation, the Display shows “Enter Password”. When the correct password is pressed in the Keypad, the lamp glows, indicating that the system is working, i.e. the door is open. The Display shows “Incorrect Password” when an incorrect password is entered. The lamp does not glow. When an incorrect password is entered more than three times, the buzzer is triggered, and it makes an audible beeping sound indicating a security breach in the system.

4.1 Hardware and Software Used

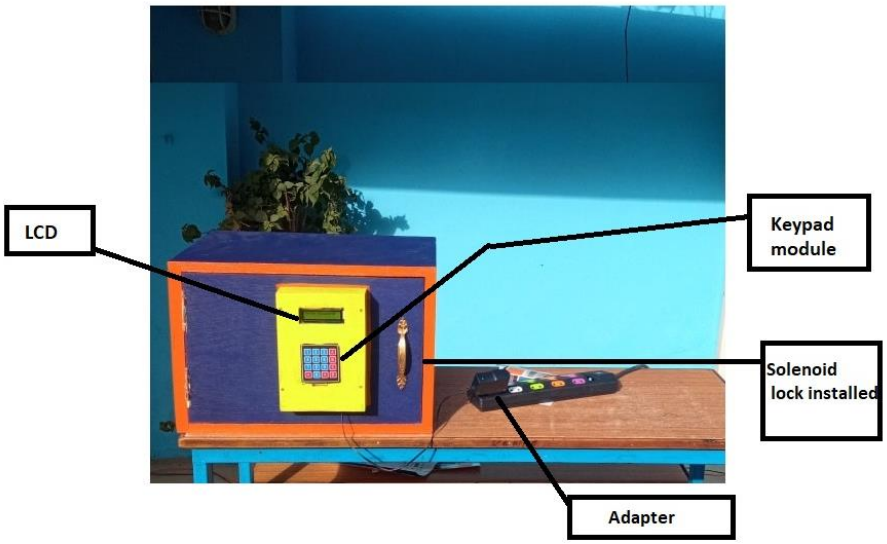

Figure 4. Password-Based Locker Prototype

The above figure shows a "Password-Based Locker Box" with the following dimension (in inches): - Length: 18 inches, Width: 12 inches and Height: 12 inches.

A 4*4 matrix Keypad is attached to the locker. This Keypad is used as an input. The user enters the required password in the Keypad, which is displayed on the LCD. A 16*2 I2C LCD is attached to the front of the locker. The LCD is used as a display for the input. A 12V power supply is required to run the system. A Solenoid Lock is attached to the back of the door. It helps in opening/closing the door as required.

In Figure 4 above, when power is supplied to the locker, the LCD displays "Enter Password:". This lets the user input the password three times until the correct one is entered after that buzzer goes high, a Blynk notification is sent as "alert unauthorized access". Thus, this makes the system highly secure and advanced.

Figure 5. Password Input Prompt

The sim 800L module connects the SIM card to the network and sends the OTP code to the respective mobile phone as defined in the program, thus helping actuate the system. A

12V adapter is used to provide supply to the system. An adapter is used to convert 12V into required 5V supply to Arduino and Relay.

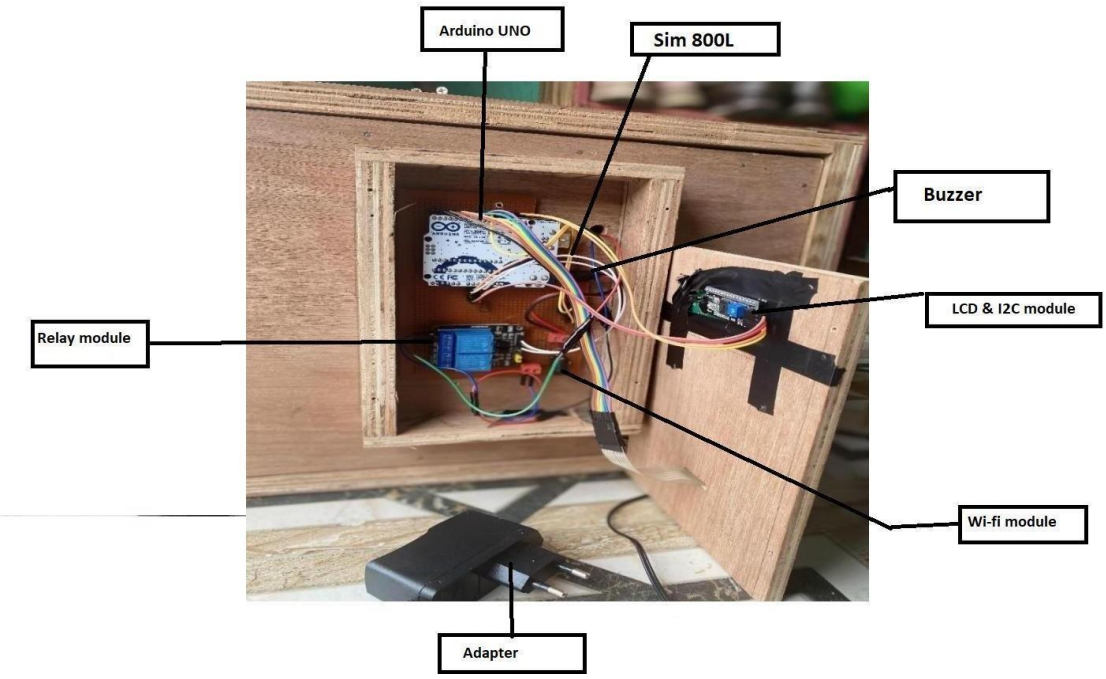

Figure 6. System Components

The Wi-Fi module allows the system to get internet access. As programmed, the system can be connected to the Blynk IoT platform for the purpose of sending the notification alert to the user. The Sim800L GSM module allows the user to get an OTP verification code in case of three wrong inputs. Thus, the OTP can be entered, and the system password can be reset to a new one.

A PCB with Arduino UNO, Relay module and Buzzer is placed in a compartment, as shown in Figure 6. The Arduino and Relay are connected to the Keypad and LCD display.

Figure 7. Display with Correct Input

The correct input prompt occurs when the user inputs the correct password, the system is set to open as relay triggers, and the solenoid lock lets the door get opened.

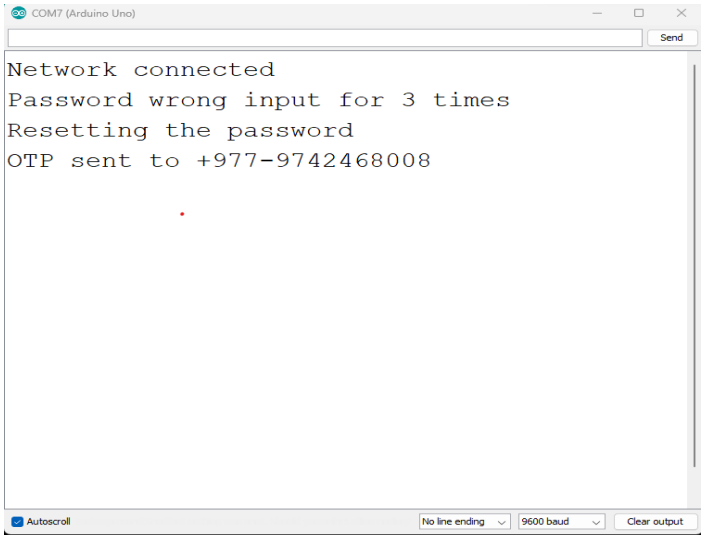

Figure 8. OTP Message Sent to the Respective Device

First, the system scans for a network using a sim 800L module and makes a connection, as in Figure 8. The OTP is sent when three invalid presses of the password are made. This would create authorized access to the system and let only the registered user enter the system and access its components inside the locker system.

The OTP verification is carried out in 4 procedures:

i) OTP sent to the registered phone number after invalid attempts are made, as illustrated in Figure 9 (a). The OTP is generated by a 'random' function in the program that generates random OTP values in specific ranges. i.e.

$$\boldsymbol{otpCode} = \boldsymbol{random}(\mathbf{100000}, \mathbf{999999});$$

Figure 9 (a). OTP Messaging to Phone

ii) OTP verification by the user is carried out as specified in Figure 9 (b). The user gets an OTP code to verify if the code matches then, a system reset can be done.

Figure 9 (b). OTP Verification Prompt

iii) Verification is checked out as illustrated in Figure 9 (c), and if the verified password is let to reset.

Figure 9 (c). OTP Verification Successful

iv) Resetting of password is allowed by the system after OTP verification is successfully done as illustrated in Figure 9 (d)

Figure 9 (d). New Password Input Prompt

The user is allowed to enter the password three times, then the wrong password prompts occur, and the user gets an OTP message as well as a Blynk notification; then, the LCD display prompts the message of enter OTP, and the user is let to enter the OTP, and if it's correct, he can reset or input a new password. When the password is entered through the keypad, if the password is correct, "Correct" will be displayed on the LCD, as shown in Figure 4.6, and the lock will be opened. After a delay of 5 seconds, the lock is triggered, and the door is locked again. In such cases, the message isn't needed for mobile phones. When incorrect input/password is entered, the locker displays "Incorrect" is shown in the display. Three tries are provided. if the correct password is not entered on three tries, the buzzer is triggered to notify a potential security breach and using a sim800L module, the OTP code is sent to the phone number defined in the program. The user can reset the password after the OTP is sent

and the user enters OTP enter part in the LCD display, and the user can finally enter OTP and reset the password.

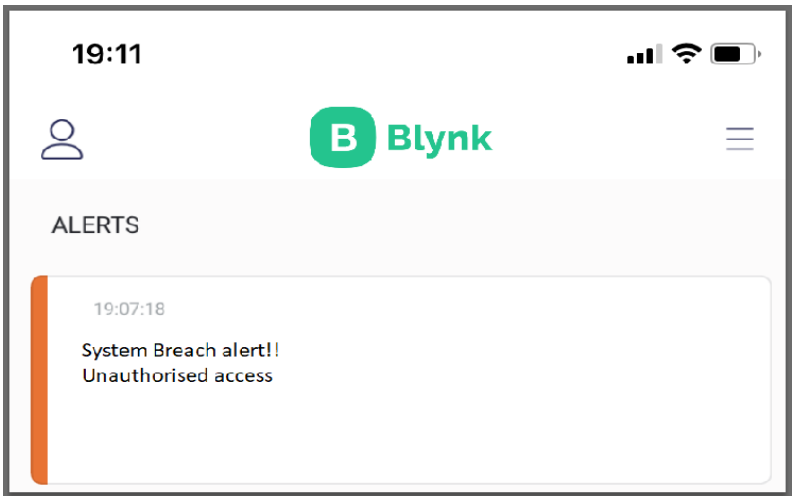

Figure 10. Blynk Notification Alert for the Wrong Password

The message through the Blynk IoT platform [15] is sent to the connected mobile phone using IoT technology, and the user is notified of any security breaches. This lets the owner get aware of possible threats to the system in the case of unauthorized access, getting a notification in the connected device as in Figure 10. This makes the security system more trustworthy to use.

4.2 Discussion

Thus, the system was perfect to avoid security breaches at different tests, and the OTP verification worked perfectly for resetting the password at three wrong inputs. The system was perfectly sending the message to the user with three passwords, and then, finally, the user could reset the password. This doesn't apply to unregistered phone numbers. The system can send the OTP verification code to the registered user and send the alert message to the user's phone using IoT Blynk technology in case of a breach. The IoT technology makes it more reliable and suited for rapid production as a product with the use of Raspberry Pi; more features can be added.

The outcomes of the research work are:

i) The OTP verification is a plus point when compared to the previous technologies of similar kind.

ii) The IoT technology makes it more reliable and supports ideas for further enhancements that can be used for fingerprint or Computer Vision systems.

iii) The system is very secure and portable with the OTP verification it is fully ready to be brought into the product level.

iv) The system needs a proper Wi-Fi connection to make it fully operatable without any problems

5. Conclusion

Every innovative work is started with a view to attending a specific motto. The main goal is to make such a type of lock security system which will provide enhanced security over traditional lock and key systems with the sacrifice of a little cost. In this regard, the proposed work is an attempt to design and implement password protected electronic lock using microcontroller Arduino UNO. A matrix keypad enters the password and unlocks the lock when the correct password is inserted. The security system available in the present market is too costly to use, especially in third-world countries like Nepal. It is quite impossible to use something so costly for the general purpose. The prototype of the proposed work enables one to make a password-protected lock, ensuring highest security at a very low cost and can be implemented easily in educational institutions. This prototype is also reliable and user-friendly. The research work was huge learning experience. In future it is possible to commercialize the locker system for the benefit of the student and institutions alike, if financial supports are extended from the institution. The use of IoT technology enhances the field of science and technology these days. These systems can be brought to product level in mass production as the system is fully fit for such a purpose.

References

[1] S. Khan and S. P. Kharde, “A Review on Smart System for Security from Theft and Other Kind of Hazard,” *International Journal of Innovative Research in Science*, vol. 7, no. 11, 2018, doi: 10.15680/IJIRSET.2018.0711036.

[2] P. Tripathi and S. Gupta, “Security metrics: Relevance in securing educational institutions,” *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, vol. 117, pp. 215–221, 2014, doi: 10.1007/978-3-319-11629-7_32/COVER.

[3] H. Andrei, V. Ion, E. Diaconu, A. Enescu, and I. Udroiu, "Energy Consumption Analysis of Security Systems for a Residential Consumer," *2019 11th International Symposium on Advanced Topics in Electrical Engineering, ATEE 2019*, Mar. 2019, doi: 10.1109/ATEE.2019.8725002.

[4] M. S. Zaghloul, "GSM-GPRS Arduino Shield (GS-001) with SIM 900 chip module in wireless data transmission system for data acquisition and control of power induction furnace," *Int J Sci Eng Res*, vol. 5, no. 4, pp. 776–780, 2014.

[5] J. F. Li, S. Cao, J. X. Duan, P. C. Gao, and Y. Hou, "A Novel Remote Monitoring and Control System Based on GSM for Home Security," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 11, no. 4, pp. 34–38, Aug. 2015, doi: 10.3991/IJOE.V11I4.4647.

[6] M. A. Hossain, N. Hossain, A. Shahid, and S. M. S. Rahman, "Security Solution of RFID Card Through Cryptography," in *International Conference on Explorations and Innovations in Engineering and Technology*, 2016.

[7] P. R. Nehete and K. P. Rane, "A Paper on OTP Based Door Lock Security System," *International Journal For Emerging Trends in Engineering and Management Research (IJETEMR)*, vol. II, no. II, pp. 21–25, Jun. 2016.

[8] N. Anusha, A. D. Sai, and B. Srikar, "Locker security system using facial recognition and One Time Password (OTP)," *Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2017*, vol. 2018-January, pp. 812–815, Feb. 2018, doi: 10.1109/WISPNET.2017.8299874.

[9] M. Lokesh, M. Giripunje, S. Sudke, P. Wadkar, and K. Ambure, "IOT Based Smart Bank Locker Security System," *SJ Impact Factor:6*, vol. 887, 2017, doi: 10.22214/ijraset.2017.11045.

[10] J. Kook, "Design and Implementation of a OTP-based IoT Digital Door-lock System and Applications," 2019.

[11] S. Mohammed and A. H. Alkeelani, "Locker Security System Using Keypad and RFID," *Proceedings of 2019 International Conference of Computer Science and Renewable Energies, ICCSRE 2019*, Jul. 2019, doi: 10.1109/ICCSRE.2019.8807588.

[12] R. R. Setyadi, Istikmal, and A. I. Irawan, "Smart Safe Prototype Based Internet of Things (IoT) with Face and Fingerprint Recognition," *2020 3rd International Seminar on Research of Information Technology and Intelligent Systems, ISRITI 2020*, pp. 394–399, Dec. 2020, doi: 10.1109/ISRITI51436.2020.9315430.

[13] Y. Yulianto, B. Juarto, I. D. A. Rachmawati, and R. Yulistiani, "Safe-Deposit Box Using Fingerprint and Blynk," *Engineering, MAthematics and Computer Science (EMACS) Journal*, vol. 4, no. 1, pp. 1–4, Feb. 2022, doi: 10.21512/EMACSJOURNAL.V4I1.8080.

[14] R. Hari Sudhan, M. Ganesh Kumar, A. U. Prakash, S. Anu, R. Devi, and P. Sathiya, "ARDUINO ATMEGA-328 MICROCONTROLLER," *INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL*, vol. 3, pp. 2321–5526, 2015, doi: 10.17148/IJIREEICE.2015.3406.

[15] "Blynk: a low-code IoT software platform for businesses and developers." https://blynk.io/ (accessed Jul. 21, 2023).

Author's biography

Biplov Paneru (https://orcid.org/0000-0003-2003-0648) is pursuing a Bachelor of Engineering in Electronics and Communication at Nepal Engineering College, Pokhara University. He has been actively engaged in Research and Development activities related to computer vision, embedded systems, image processing, etc. He is a research and development engineer in rocketry at the National Innovation Center of Nepal and a freelance software developer on Upwork. This research was conducted as part of the product development process, and its prototype was successfully created and implemented.

Krishna Bikram Shah (https://orcid.org/0000-0003-1763-511X) is an accomplished Assistant Professor in the Computer Science and Engineering department at Nepal Engineering College. With a strong publication record in international journals and active participation in projects like InterNepInd, B+NeSDG (Co-funded by Erasmus+), Krishna's research contributions encompass a wide range of areas, including Artificial Intelligence, Machine Learning, Image Processing, IoT, renewable energy

and SDGs. With a dedication to academic excellence and a passion for innovation, Krishna's work continues to advance the field of computer science and engineering, offering valuable insights and solutions for real-world challenges.

Bishwash Paneru is pursuing a Bachelor of Engineering in Chemical Engineering at Institute of Engineering, Pulchowk Campus. He has been actively engaged in Research and Development activities related to fuel conversion, green hydrogen, pyrolysis, water treatment, Machine Learning etc. He is a research intern at Environ Renewables and has been researching in field of green hydrogen, ML algorithms and alternative energy. He is also a chemical engineering freelancer at upwork.