IRO Journal on Sustainable Wireless Systems (ISSN: 2582-3167)
www.irojournals.com/irosws/

Password based Smart Doorlock System using Arduino UNO for Enhanced Security

S. Vinodhini[1], Gnanavarshini S[2], Sheryl Eby[3], Divya Prapanjani PA[4]

[1]Assistant professor, Department Information Technology, Velammal Engineering College, Tamil Nadu, India

[2]Students, Department Information Technology, Velammal Engineering College, Tamil Nadu, India

E-mail: [1]vinodhini@velammal.edu.in, [2]gnvarshinisiva@gmail.com, [3]sheryleby21@gmail.com, [4]divya17429@gmail.com

Abstract

In recent years, the demand for secure access systems has increased significantly, especially in residential and commercial areas. Hence, this presents the design and implementation of a password-based door lock system using an Arduino microcontroller and a servo motor. The system provides a cost-effective and reliable solution for managing access to physical sites. The proposed system uses an Arduino microcontroller as the central device to control the authentication process and to control the servo motor that operates the door locking mechanism. A matrix keyboard is used to enter the password, which provides a user-friendly interface for communication. The servo motor is responsible for physically locking and unlocking the door mechanism based on the authentication result. The operational workflow of the system requires the user to enter a predetermined password using a keyboard. The Arduino microcontroller compares the entered password with the password stored in its memory. After successful authentication, a servo motor is operated to open the door, allowing access to the authorized person. Conversely, failed authentication will result in access being denied.

Keywords: Arduino UNO, 4*4 Keypad lock, Security, Servomotor

DOI: https://doi.org/10.36548/jsws.2024.2.002
Received: 20.03.2024, received in revised form: 21.04.2024, accepted: 11.05.2024, published: 21-05-2024

1. Introduction

In today's scientific environment, protection has become a top concern, in home, commercial, and industrial areas. Old lock and key systems are being replaced by smarter and more efficient access control structures for greater security and convenience. Among these, password-based locks are top-selling due to their simplicity, dependability, and effectiveness. Therefore, we present the design and implementation of an identification lock system using an Arduino microcontroller and a servo motor. This system provides a new approach to access control by integrating the integrity of Arduino-based programming with the mechanical efficiency of servo motors, offering a reliable and easy-to-use solution for site access control. Using the estimating capacity and flexibility of Arduino, we aim to design an entrance-to-room locking system that is not only effective in terms of protection but also accessible to people with various technical abilities. Servo motors serve as the mechanical link between the digital verification process and the physical locking mechanism of the entrance to a room. Their precision and ability to move within a defined range make them a suitable choice for implementing a locking mechanism based on the verification results generated by the Arduino microcontroller. Incorporating an identification verification system adds a layer of flexibility to the process, allowing authorized individuals to gain access by entering a predefined identification code through a connected keyboard. This intuitive interaction model makes the system convenient while maintaining security measures to prevent unauthorized access.

We carefully analyze design concepts, component fittings, programming procedures, and system layout to visualize and validate the effectiveness and reliability of the proposed system in real-world scenarios. In summary, our aim is to contribute to the ongoing discussion of modern access control solutions by providing a practical and scalable alternative that capitalizes on its efficient features. This project focuses on integrating Arduino and servo motor electronics to offer an alternative to traditional entrance locking procedures, effectively bridging the gap between digital and physical verification methods, thereby enhancing security and usability across various environments.

1.1 Applications of the System

For home security, implementing a password-protected door lock system can improve home security by limiting access to only authorized individuals. For office security, offices can

use such systems to control access to restricted areas of the premises, ensuring that only authorized persons enter. For laboratory access control, research laboratories and facilities benefit from a password-based door locking system that controls access to sensitive equipment and materials. For classroom security, schools and educational institutions can use these systems to secure classrooms and prevent unauthorized access during class. For security of storage units, storage units can be equipped with password protected locks to protect valuables and prevent theft. For gyms, sports clubs and entertainment facilities can use these systems to protect locker rooms and ensure the safety of merchandise. For access to hotel rooms, hotels can use password-based locking systems to secure access to rooms, improving guest security and privacy. For server room access, server centers and IT facilities can use these systems to control access to server rooms and prevent unauthorized entry. For retail security, retailers can use password-based door locking systems to protect back rooms, warehouses or offices. For garage door entry, homeowners can implement these systems to secure their garage doors and prevent unauthorized access to their homes.

2. Related Work

The project focuses on the design and development of password-based smart door lock system equipped with IoT technology for enhanced safety, security and functionality. Goswami et al. (2017) introduced an automated password-protected door lock system, laying the groundwork for our project by exploring the fundamental concepts of password-based security mechanisms [1]. Motwani et al. (2021) conducted a comprehensive review of multifactor door locking systems, shedding light on the importance of incorporating multiple authentication factors for enhanced security [2]. Rahman et al. (2018) proposed a password-protected electronic lock system tailored for smart home security, providing insights into the integration of such systems into broader home automation frameworks [3]. Rane (2015) explored the integration of GSM technology with password-based door locking systems, highlighting the potential for remote access and control [4]. Ray (2022) further delved into the intricacies of password-based door lock systems, contributing insights into system design and implementation considerations [5]. Sia et al. (2022) introduced a voice-activated storage locker designed for visually impaired individuals, showcasing innovative approaches to access control beyond traditional keypad-based systems [6]. Vadakkan et al. (2021) presented a study on door locking using keypads and Arduino, emphasizing the practical implementation aspects of such

systems [7]. Vamsi et al. (2019) explored face recognition-based door unlocking systems using Raspberry Pi, offering alternative approaches to biometric-based access control [8].

Verma and Tripathi (2010) presented a digital security system integrating RFID technology for door lock systems, offering insights into the application of RFID in access control [9]. Shafin et al. (2015) contributed to the discourse with the development of an RFID-based access control system, emphasizing practical implementations tailored to specific contexts such as Bangladesh [10]. Hassan et al. (2012) explored face recognition-based door lock systems using microcontrollers, showcasing advancements in biometric authentication for access control [11]. Madhusudhan and Shankaraiah (2015) implemented an automated door unlocking and security system, underscoring the importance of seamless integration and user-friendly interfaces [12]. Chowdhury (2011) introduced biometrics as a revolutionary authentication process, highlighting the potential for enhanced security through physiological characteristics [13]. Jagdale et al. (2016) conducted a review on intelligent locker systems, emphasizing the role of cryptography, wireless, and embedded technologies in access control solutions [14]. Chen et al. (2016) proposed intelligent locks based on the triple KeeLoq algorithm, showcasing advancements in cryptographic-based security mechanisms [16]. Furthermore, Johnson and Dow (2016) patented an intelligent door lock system with encryption, offering innovative solutions to bolster security measures [17]. The use of IOT can further enhance the security process [15] but the proposed work by synthesizing insights from these diverse studies, aims to develop a robust and secure password-based door lock system leveraging Arduino, servo motor and keypad membrane technology, contributing to the advancement of access control solutions in various domains and aims to integrate it in the future work.

3. Proposed Work

3.1 Overview

The password-based smart door lock system utilizes Arduino UNO, a servo motor, and a keypad membrane. This system aims to provide a secure and convenient method for controlling access to doors or other entry points. The Arduino UNO serves as the central control unit, managing the input from the keypad membrane, processing the password entered by the user, and triggering the servo motor to actuate the locking mechanism accordingly. The keypad

membrane acts as the interface through which users can input their passwords, offering a user-friendly and intuitive means of interaction. The servo motor is responsible for physically locking and unlocking the door mechanism in response to the correct password being entered. Additionally, we aim to explore potential enhancements such as incorporating encryption algorithms for password security or integrating additional sensors for enhanced functionality. Overall, the proposed work seeks to develop a robust and versatile password-based door lock system using readily available components and open-source technologies, with the goal of providing a highly secured accessible controls in various settings.

3.2 Methodology

Arduino UNO

Arduino could be a prototyping board (open boot) that smoothly installs usable devices and software as of in Figure.1. It has a programmable inspired disturbance (like a microcontroller) and a non-financial spreadsheet called the Arduino IDE (Coordinates Advancement Environment) which is used to print the calculation law and upload it to the canvas board. Arduino pages can determine parallel or numerical feedback signals from different sensors and turn the bureaucracy into a sum within motor function, on and off, cloud ratio and many accompanying capabilities. You can control the power of your board by sending a bunch of data to the internal microcontroller using the Arduino IDE (called a bootloader). Unlike most early programmable circuits, the Arduino does not require additional connectors (called a computer manager) to stack unused chips on the board. You can use the USB cable as it was. In addition, the Arduino IDE uses a more streamlined variant of C++, which makes the data calculation smooth. Finally, Arduino provides a standard framework specification that breaks down the advantages of a microcontroller into a more responsive unit. There are various Arduino pages that suddenly disappear due to the microcontrollers used. Be that as it may, all Arduino boards also agree: they are calculated using the Arduino IDE. The differences are the number of inputs and outputs (the number of sensors, LEDs and buttons on the ID card), speed, physical performance, form factor, etc. It comes with some sheets and lacks a priority interface

(accessories) that you would have to buy yourself. Some can run directly from 3.7V, while a conceivable choice request is not quite 5V.

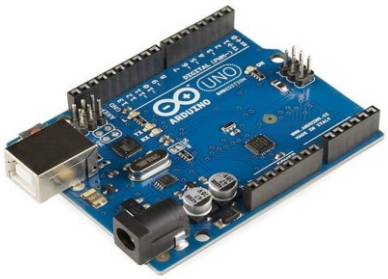

Figure 1. Arduino

Servo Motor

A servo motor is an energetic engine designed for precise control of position, speed, and movement as of in Figure.2. It operates using independent-loop control, where the motor's position is continuously adjusted based on feedback from a position sensor to ensure accurate positioning. A typical servomotor system consists of a rotor within a stator that creates a magnetic field when an electric current is applied. This magnetic field causes the rotor to move and align with the desired position. The position sensor provides feedback to the controller, which compares the actual position with the desired position and adjusts the motor accordingly. This feedback mechanism enables servo motors to achieve high levels of accuracy and repeatability, making them essential in various applications such as robotics, CNC machines, aerospace systems, and automation.

Figure 2. Servo Motor

9V Battery

A 9V battery is a little, compact control supply regularly utilized in convenient electronic gadgets such as smoke finders, farther controls and guitar pedals as of in Figure.3.

It as a rule comprises of six round and hollow or rectangular components associated in arrangement to give a add up to voltage of almost 9 volts. Each cell comprises of a cathode (positive post), an anode (negative post) and an electrolyte arrangement that encourages the development of particles between the anodes. The working component of a 9V battery includes a chemical response called oxidation-reduction, where electrons are exchanged between the anode and cathode through an outside circuit, producing power. In this prepare, the anode is oxidized, discharging electrons, whereas the cathode is diminished and acknowledges electrons. This stream of electrons makes an electric current that can control different electronic gadgets. As the battery releases, the chemicals interior continuously release, diminishing its voltage until it comes to a point where it can no longer give sufficient current, requiring substitution or energizing with rechargeable forms.

Figure 3. 9V Battery

Jumper Wires

Jumper wires are critical component in hardware and prototyping, comprising of protects wires with connectors on both closes as of in Figure.4. These connectors are more often than not male, female, or croc connectors that permit simple and secure association between different electronic components such as breadboards, microcontrollers, sensors, and other peripherals. The instrument behind jumper wires includes exchanging electrical signals and control between components. When embedded into suitable attachments or pins, jumpers shape electrical progression, permitting signals and current to stream through the circuit. Their adaptability and flexibility make them important for fast prototyping and testing of electronic circuits, as they encourage the creation of transitory associations without patching. Jumper wires come in diverse lengths, colors and sizes to suit distinctive applications and inclinations, giving a helpful and productive arrangement for wiring and interfacing components in electronics.

Figure 4. Jumper wires

4*4 Keypad Membrane

A 4x4 keypad membrane switch is a sort of input gadget commonly utilized in electronic frameworks to give a client interface for entering numeric or alphanumeric information as of in Figure.5. It comprises of a lean adaptable layer with conductive follows printed on its surface and organized in a lattice of four lines and four columns. Each crossing point of lines and columns shapes a key position. Over those intersections are dome-shaped touch switches made of conductive fabric. When the key is squeezed, it interfaces the comparing push and column follows and closes the circle. This alter in conductivity is identified by the system's microcontroller or interface, which at that point deciphers the squeezed key based on the gotten push and column signals. The layer exchanging instrument of the 4x4 console is based on the distortion of the dome-shaped buttons to make an electrical contact that gives the client a sense of touch. This demonstrate offers a compact, reasonable and solid arrangement for entering information into different electronic gadgets such as calculators, inaccessible controls and security frameworks. The circuit diagram is illustrated in Figure.6.

Figure 5. 4*4 Keypad Membrane

3.3 Circuit Diagram

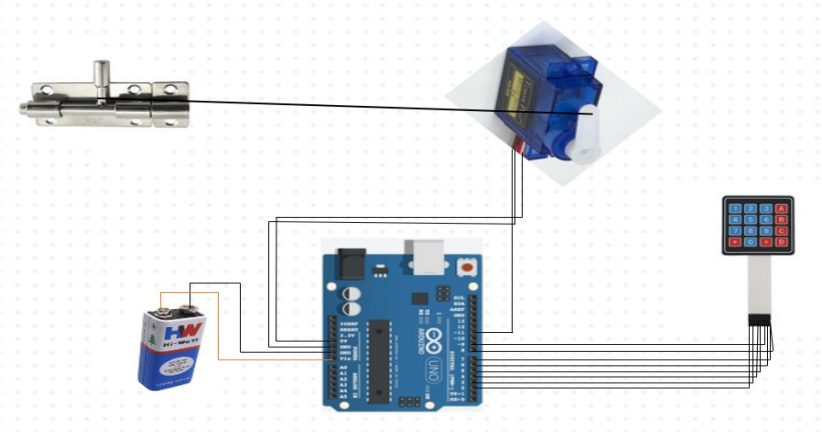

Figure 6. Password based Smart Door Lock System Diagram

3.4 Hardware Connections

a. Interfacing Servo Motor with Arduino

Figure.7 depicts that the servo motor's three wires was connected to the Arduino board: the red wire to the 5V pin for power, the brown wire to the GND pin and the orange wire to the pin 11 of Arduino. Then in the Arduino code, the servo library is used to control the motor's position and movement by specifying the desired angles (90 deg to the left to open and 90 deg to the right to close). Finally, the code was uploaded to the Arduino board and powered it up using USB cable to see the servo motor in action.

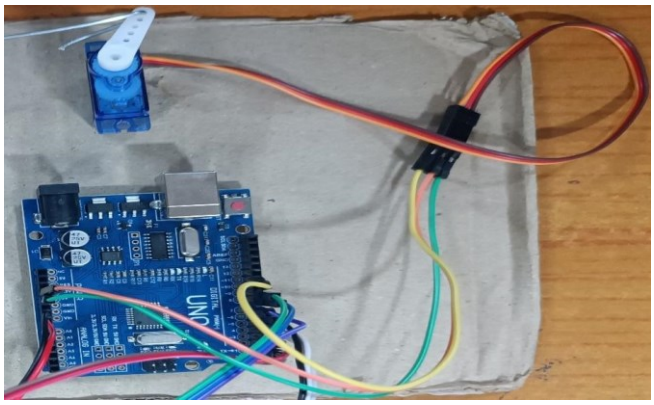

Figure 7. Interfacing Servo Motor with Arduino

b. Interfacing Keypad with Arduino

Figure.8 depicts that the keypad's row pins (8,7,6,5) are connected to (2,3,4,5) of Arduino's digital pins and column pins (4,3,2,1) are connected to (9,6,7,8) of Arduino's digital pins using jumper wires. The keypad's rows and columns are connected to digital pins using a matrix configuration. Then, the keypad library is used in Arduino to interface with keypad, allowing for input detection. Finally, the code was uploaded to interpret the keypad inputs and perform desired actions based on user input.

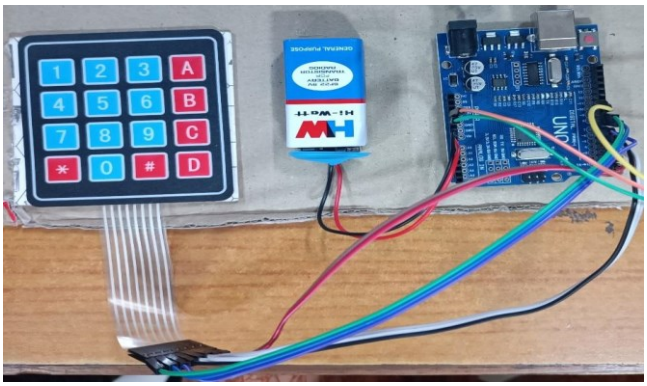

Figure 8. Interfacing Keypad with Arduino

c. Interfacing 9V Battery with Arduino

Figure.9 depicts that a 9V battery is connected to an Arduino UNO board by attaching the positive terminal of the battery to the Vin pin and the negative terminal to the GND pin. A stable power supply is ensured without relying solely on USB connection. This setup enables portability and flexibility for the system, allowing them to function independently of a computer or external power source.

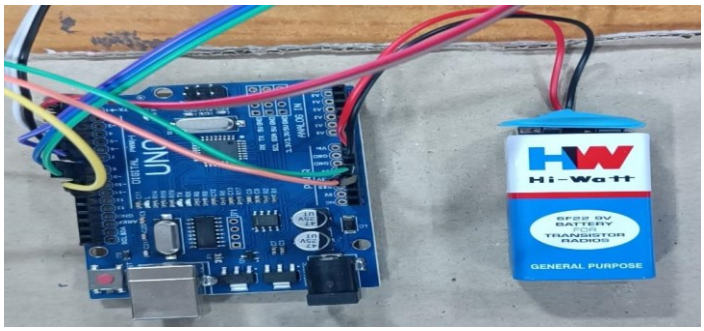

Figure 9. Interfacing 9V Battery with Arduino

d. Interfacing Lock with Servo

Figure.10 depicts that a lock was integrated with the shaft of the servo motor for open and close actions ensuring proper alignment and stability of the connection between servo motor and the lock for reliable operation. The servo motor's rotational motion was then controlled using an Arduino. By programming the servo to rotate to specific angles, it can lock or unlock the mechanism, provides secure access control.

Figure 10. Interfacing Lock with Servo

e. Complete Connections

Figure.11 depicts that the complete system was designed with an Arduino UNO, servo motor, keypad membrane, and a 9V battery, and then the code for the system was uploaded to the Arduino board using a USB cable from the Arduino IDE. The code for the servo motor and keypad was written. After uploading the code onto the Arduino board, the USB cable was removed, and the system was now ready to test. If any changes need to be made to the code, then erase the previous uploaded code from the Arduino board by pressing the red button and upload the new code into it.

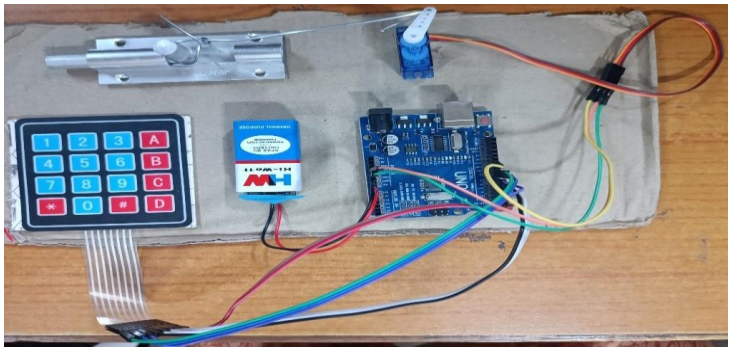

Figure 11. Complete Connection

4. Results and Discussion

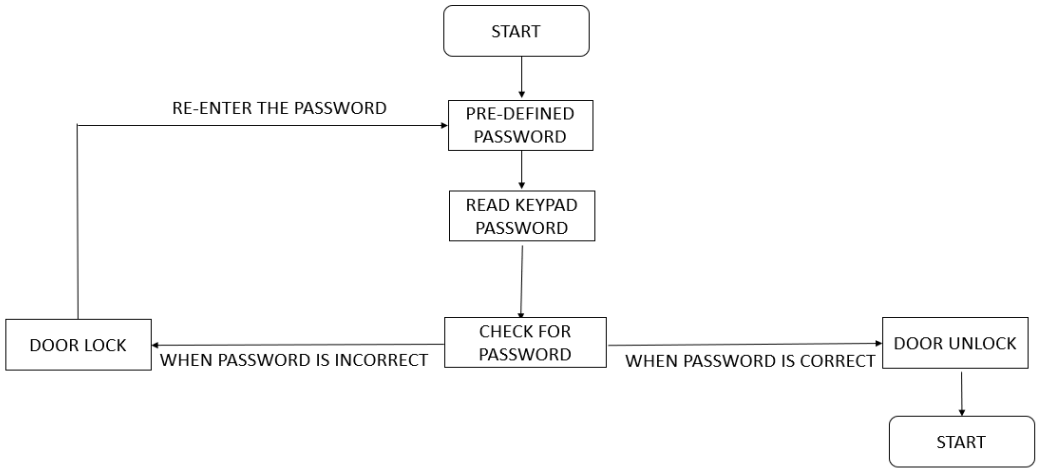

Figure 12. Proposed System's workflow

The password-based entry latch framework uses an Arduino UNO microcontroller and servo motor, a 9V battery, a 4x4 keyboard membrane, and a physical latch. The Figure 12 illustrates the work flow of the proposed. The framework works as follows:

Figure 13. Door Closed

Figure 14. Door Opened

Initialization: Arduino UNO is modified to initialize the servo motor, keyboard membrane, and characterize the control password.

Customer Entry: When the customer approaches the entrance, they will be asked to enter a password using the 4x4 keyboard membrane.

Keyboard Input Maintenance: When a customer enters a password, the Arduino UNO examines the input of the keyboard membrane.

Comparison: When the client finishes entering the password, the Arduino will compare it with the predefined password.

Confirmation: If the entered password matches the repair password, the Arduino will send the ticket to the servo motor.

Servo Operation: A servo motor rotates to a predetermined point when a ticket is received, which opens the entry mechanism.

Entrance Open: When the servo motor rotates, the entrance hook is pulled out, allowing the customer to open the door.

Password Processing Off-Base: If the entered password does not match the predefined password, no flag will be sent to the Arduino servo engine.

Latch State: So, the servomotor remains inert and the gateway is locked.

In general, this framework provides a secure and computational strategy to unlock the gateway using a password entered through the keyboard layer. This ensures that customers authorized with a repair password can access locked areas, improving security and convenience.

5. Future Works and Conclusion

Enabling the creation of multiple user profiles with unique passwords or biometric data, allowing for customized access permissions for different individuals. Incorporate sensors or alarms to detect and deter tampering attempts, such as forced entry or manipulation of the locking mechanism. In future developments, we intend to integrate an LCD display into the system to provide informative feedback to users. This display will be utilized to convey messages such as "Password is correct" upon successful authentication, "Password is incorrect" if an incorrect password is entered, and "Please enter the correct password" to prompt users to retry. The implementation of a password-based door lock system using Arduino UNO, servo motor, 9V battery, and keypad membrane represents a significant advancement in home security technology. By harnessing the power of microcontrollers and electromechanical components, this system provides a reliable and customizable solution for controlling access to residential or commercial spaces. The utilization of Arduino UNO as the central processing

unit allows for flexibility in programming and integrating additional features, enhancing the overall functionality of the system. The servo motor's precise control enables seamless unlocking of the door upon successful authentication, offering convenience to authorized users. Moreover, the integration of a 9V battery ensures uninterrupted operation even during power outages, ensuring continuous protection. The inclusion of a keypad membrane provides a user-friendly interface for inputting passwords, making the system accessible to a wide range of users. Overall, this system not only enhances security but also offers ease of use and adaptability, making it a valuable addition to modern door access control systems. With further development and refinement, password-based door lock systems have the potential to revolutionize home security measures and contribute to safer living environments.

References

[1] Goswami, S., Choudhury, A., Das, S., Banerjee, T., & Ghosh, S. (2017). Automated password protected door lock system. Advances in Industrial Engineering and Management, 6(1), 48-52.

[2] Motwani, Y., Seth, S., Dixit, D., Bagubali, A., & Rajesh, R. (2021). Multifactor door locking systems: A review. Materials Today: Proceedings, 46, 7973-7979.

[3] Rahman, M. M., Ali, M. S., & Akther, M. S. (2018). Password Protected Electronic Lock System for Smart Home Security. International Journal of Engineering Research and Technology, 7(4), 541-544.

[4] Rane, C. (2015). Password Based Door Locking System Using GSM. International Journal of Engineering Trends and Applications (IJETA), 2(4), 48-53.

[5] Ray, I. (2022) Password based door lock system. International Research Journal of Modernization in Engineering Technology and Science, 4(5), 2405-2413.

[6] Sia, B. J., Wong, W. K., & Min, T. S. (2022, April). Voice Activated Storage Locker for Visually Impaired. In 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI) (pp.442-447). IEEE.

[7] Vadakkan, A., Babu, A. V. K., Pappachan, C. and Sunny, A. (2021) Door locking using keypad and ARDUINO. International Research Journal of Modernization in Engineering Technology and Science, 3(11), 780-787.

[8] Vamsi, T.K., Sai, K.C., & Vijayalakshmi, M. (2019). Face recognition based door unlocking system using Raspberry Pi. International Journal of Advance Research, Ideas and Innovations in Technology, 5(2), 1320-1324.

[9] Gyanendra K Verma and Pawan Tripathi, “A digital security system with door lock system using RFID technology”, International Journal of Computer Application, Volume 5–No.11, pp. 6-8, August 2010.

[10] M. K. Shafin, K. L. Kabir, N. Hasan, “Development of an RFID based access control system in the context of Bangladesh”, IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems, pp. 1-5, 2015.

[11] H. Hassan, R. A. Bakar, A. T. F. Mokhtar, “Face recognition based on auto switching magnetic door lock system using micro-controller”, International Conference on System Engineering and Technology, pp. 1-6, 2012.

[12] Madhusudhan M. and Shankaraiah,“Implementation of automated door unlocking and security system”, International Journal of Computer Applications, pp. 5-8, 2015.

[13] Arundhuti Chowdhury, “Revolution in authentication process by using biometrics”, International Conference on Recent Trends in Information Systems, pp. 36-41, 2011.

[14] R. Jagdale, S. Koli, S. Kadam and S. Gurav, “Review on intelligent locker system based on cryptography, wireless & embedded technology”, International Journal of Technical Research and Applications, pp. 75-77, March 2016.

[15] CM Nalayini, P Sreemathi, B Nanditha, "Deterrence of Accident Using IoT",Journal of Trends in Computer Science and Smart Technology(ISSN: 2582-4104), Volume 4, Issue 2, pp 96-105, July 2022, Inventive Research Organization

[16] H. Chen, J. Liu and C. F.Yang, “Design of intelligent locks based on the triple KeeLoq algorithm,”Advances in Mechanical Engineering, vol. 8, no. 4, pp. 1-7, 2016.

[17] Jason Johnson and Christopher Dow, “Intelligent door lock system with encryption”, US Patent Application Publication Johnson et al., pp. 1-92, June 2016.