Development of a Microcontroller-Based Advanced Control System for Secure Door Locking

Md. Mayn Uddin

Dept. of Electrical and Electronic Engineering, Jatiya Kabi Kazi Nazrul Islam University, Trishal, Mymensingh, Bangladesh

---***---

Abstract - *Security is a crucial requirement in modern access control systems, and this project presents a password-based door locking security system to enhance protection. The system utilizes a microcontroller to authenticate user input from a keypad and grants access only when the entered password matches the stored password in memory. If the password is correct, the door unlocks; otherwise, access is denied. An LED indicator is included to provide visual feedback regarding authentication status, improving user interaction and system usability. This embedded security solution offers a low-cost, efficient, and reliable method for preventing unauthorized entry. It can be implemented in doors, lockers, and other restricted access systems, making it suitable for various security applications. By employing microcontroller-based authentication, the system ensures enhanced safety and operational efficiency in modern security environments.*

***Key Words*: Arduino UNO R3, LCD Display, Buzzer, IR Sensor.**

1. INTRODUCTION

Security has become one of the most important concerns in modern society. With the increasing number of security threats, theft, and unauthorized access incidents, ensuring the safety of homes, offices, laboratories, and other restricted areas has become a major priority [1],[2]. Access control systems play a vital role in maintaining security by regulating who can enter or exit a particular location. For many years, traditional mechanical door lock systems have been widely used for this purpose. However, these systems have several limitations that make them less reliable in the modern era. Mechanical keys can easily be lost, stolen, or duplicated, and the locks themselves can be damaged or forced open using simple tools [3]. These vulnerabilities highlight the need for more secure, efficient, and intelligent locking mechanisms. With the rapid advancement of electronics, digital technology, and embedded systems, modern security solutions have evolved significantly. Electronic door lock systems are increasingly being adopted because they provide enhanced security, flexibility, and convenience compared to conventional locking methods [4]. Among these solutions, integrated door lock security systems have gained significant attention due to their ability to combine multiple technologies into a single framework. Such systems integrate microcontrollers, sensors, input devices, and alert mechanisms to create a smart and automated security environment. An integrated door lock security system typically operates by verifying the identity of the user through an authentication method such as a password, code, or digital key. In this project, a microcontroller-based system is used to manage the entire door locking and unlocking process. The user enters a password using an input device such as a keypad, and the microcontroller compares the entered code with the stored password in the system memory [5]. If the password is correct, the door unlocking mechanism is activated and the user is granted access to the secured area. On the other hand, if an incorrect password is entered, the system denies access and may activate an alarm or warning signal to indicate an unauthorized attempt. The integration of additional modules such as sensors, displays, and alarm systems further enhances the functionality and effectiveness of the security system. Sensors can detect the presence of individuals near the door, while display units such as LCD screens can provide instructions or status messages to users. Alarm systems, such as buzzers, can notify occupants of suspicious activities or repeated incorrect password attempts. These integrated features help create a more reliable and user-friendly security solution[6],[7]. Another important advantage of an integrated door lock system is its flexibility. Unlike traditional locks, electronic systems allow the password or access code to be easily changed or updated without replacing physical components. This makes the system more adaptable to different users and changing security requirements. Furthermore, such systems can be designed to include additional security features, such as limiting the number of incorrect password attempts, temporarily disabling the system after repeated failures, or keeping a record of access attempts. The development of integrated security systems also supports the growing concept of smart homes and automated buildings. As technology continues to evolve, security systems are becoming more intelligent, efficient, and interconnected with other devices. An integrated door lock security system represents an important step toward modernizing access control mechanisms and improving overall safety. Therefore, the design and implementation of an integrated door lock security system not only enhance security but also provides a convenient, reliable, and cost-effective solution for modern access control applications. Such systems have wide applications in residential buildings, offices, laboratories, banks, and other environments where controlled and secure access is essential.

2.BASIC COMPONENTS AND SYSTEM ARCHITECTURE

This section provides a brief description of the circuit components used in the system. It explains the features and applications of each component involved in the project. The Arduino is used as the main controller for building and managing the electronic circuit. It consists of a programmable microcontroller board that can be easily connected to a computer through a USB interface. The Arduino platform simplifies the design of electronic systems by integrating both hardware and software functionalities. The programming language used in Arduino is based on a simplified version of C++, which makes it easier to write and understand the code. Using Arduino allows complex electronic circuits to be controlled efficiently with minimal wiring and simplified programming.

Arduino UNO: The Arduino Uno R3 shown in figure 1 is a microcontroller board based on a removable, dual-inline-package (DIP) ATmega328 AVR microcontroller. It has 20 digital input/output pins (of which 6 can be used as PWM outputs and 6 can be used as analog inputs). Programs can be loaded on to it from the easy-to-use Arduino computer program. The Arduino has an extensive support community, which makes it a very easy way to get started working with embedded electronics. The R3 is the third, and latest, revision of the Arduino Uno. The Arduino Uno is a microcontroller board based on the ATmega328. It has 20 digital input/output pins (of which 6 can be used as PWM outputs and 6 can be used as analog inputs), a 16 MHz resonator, a USB connection, a power jack, an in-circuit system programming (ICSP) header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer (or appropriate wall power adapter) with a USB cable or power it with a AC-to-DC adapter or battery to get started[8].

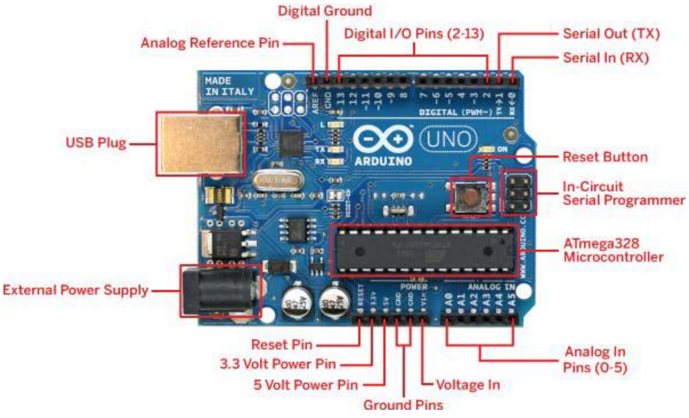

Fig 1: Arduino UNO

LCD: Here we are using a 16×2 L.C.D which is a dot matrix Liquid Crystal Display shown in figure 2. Its function is to display the alphanumeric symbols to indicate the status message of the circuit. This circuit can display the two lines and each line contains 16 characters. This L.C.D contains an internal oscillator circuit to work in synchronization with the controller.

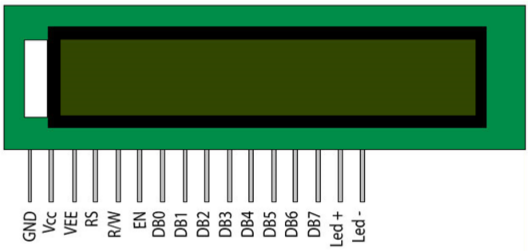

Fig 2: LCD Display

4×4 Matrix Keyboard: The keyboard used in this system is arranged in a matrix format, where rows and columns are connected to the pins of the microcontroller. It consists of push buttons containing numbers from 0 to 9, alphabets from A to D, an Enter button, and an Escape button. This keypad allows users to input the password required for unlocking the door. When a key is pressed, the corresponding row and column signals are detected by the microcontroller, which interprets the input and processes it for authentication[9].

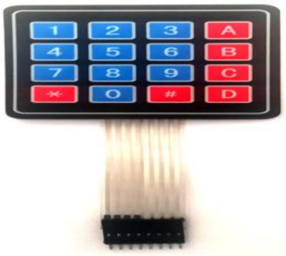

Fig 3: A 4×4 Matrix Keyboard

Buzzer or any Alarming Circuit: The buzzer is based on a piezoelectric material that converts electrical signals into mechanical vibrations. These vibrations are amplified to produce a buzzing sound, which serves as an indication of an incorrect password entry or unauthorized access attempt. The alarming circuit is used to alert users about security breaches or wrong inputs. Instead of a buzzer, various other indication methods can also be implemented, such as LED indicators, display messages, or visual alert systems, depending on the system requirements[10].

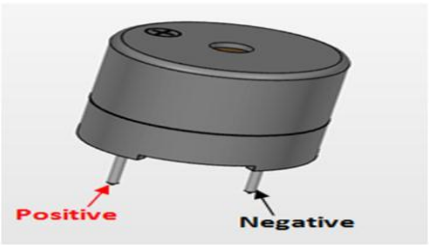

Fig 4: Buzzer

IR Sensor: An infrared (IR) sensor is an electronic device used to detect objects and measure motion by sensing infrared radiation shown in figure 5. It works on the principle that all objects emit thermal radiation, which is invisible to the human eye but detectable by the sensor. The sensor consists of an IR LED that emits infrared light and a photodiode that receives the reflected light from nearby objects. When infrared light falls on the photodiode, its resistance and output voltage change, allowing object detection within a typical range of 10–30 cm. This sensor is widely used for proximity detection and security applications where motion or object presence needs to be identified[11],[12].

Fig 5: IR sensor

A light-emitting diode (LED): A light-emitting diode (LED) is a semiconductor device that emits light when electric current passes through it through electroluminescence. It is widely used in electronic systems due to its low power consumption, long life, and high efficiency[13],[14]. In this project, the LED serves as a visual indicator of system status. It lights up when the correct password is entered, signaling successful authentication and door unlocking, while remaining off or indicating an error for incorrect input. This provides immediate feedback to the user without requiring additional displays, enhancing system usability and reliability.

2.1 System Flowchart

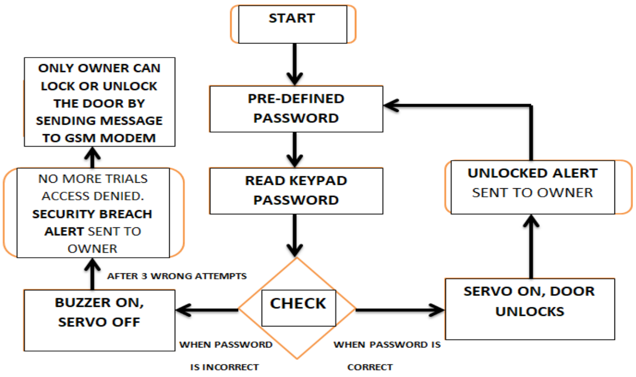
START
PRE-DEFINED PASSWORD
READ KEYPAD PASSWORD
CHECK
WHEN PASSWORD IS INCORRECT
WHEN PASSWORD IS CORRECT
BUZZER ON, SERVO OFF
SERVO ON, DOOR UNLOCKS
UNLOCKED ALERT SENT TO OWNER
AFTER 3 WRONG ATTEMPTS
NO MORE TRIALS ACCESS DENIED. SECURITY BREACH ALERT SENT TO OWNER
ONLY OWNER CAN LOCK OR UNLOCK THE DOOR BY SENDING MESSAGE TO GSM MODEM

Fig 6: System Flowchart**.**

The flowchart illustrates in figure 6, the working principle of the door lock security system. Initially, the system starts in a locked state with a predefined password stored in its memory. When the device is powered on, it resets and prompts the user to enter the password through the keypad. The entered password is read by the Arduino Uno, which compares it with the stored password. If the password matches, the system grants access and unlocks the door for a limited period of time, after which it automatically locks again to maintain security. If the password is incorrect, the system activates the buzzer as an alarm signal to indicate an unauthorized attempt. After three wrong attempts, the system may disable further input or temporarily lock itself for security purposes. Additionally, the system provides real-time feedback through an LCD display, showing messages such as “Access Granted” or “Wrong Password.” The owner also receives notifications about the door’s locking and unlocking status. Thus, the flowchart represents a simple yet effective security mechanism that combines password authentication, automated door control, and alert systems to enhance security and prevent unauthorized access.

2.2 Our Proposed Model

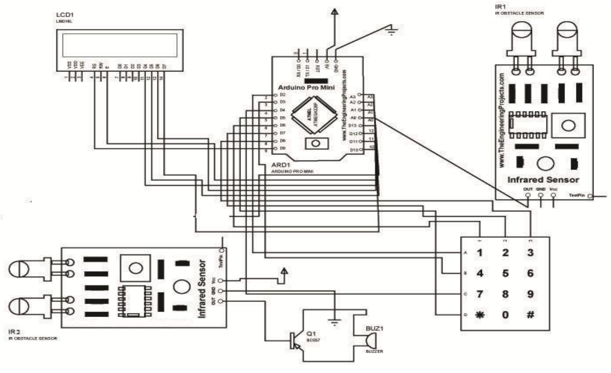

Fig 7: Proposed model.

The diagram illustrates in figure 7 a microcontroller-based security system in which different peripherals such as a keypad, infrared sensor, and output devices are interconnected with the control unit. The keypad is used for password entry; its data lines are connected to the microcontroller so that the entered code can be read and compared with the stored password. If the password matches, the controller activates the output section typically a relay or motor driver to unlock or open the door. An infrared sensor is also connected to the controller, which detects the presence of an object or person and provides input to the system for additional security or automation. The relay or actuator is driven by the controller’s output pins, allowing high-power devices such as a door lock to be switched on or off. Power supply connections are distributed to all modules to ensure proper operation. Overall, the system functions as an electronic door lock where user authentication through the keypad and sensor input determines whether access is granted.

3. RESULT AND DISCUSSION

The developed door lock security system successfully demonstrates a low-cost and efficient method for enhancing security using microcontroller-based control. The system allows authorized access through a password-based mechanism, ensuring that only users with the correct credentials can unlock the door. Experimental results indicate that the system responds accurately to valid inputs and denies access to incorrect passwords, thereby providing fundamental security functionality. However, the system operates within a limited range and does not support remote access, which restricts its usability in applications requiring wireless or internet-based control. Furthermore, if the user forgets the password, there is no alternative recovery mechanism, making password management crucial for continuous operation. Despite these limitations, the project achieves its primary objective of providing a secure and automated door locking mechanism. The integration of microcontroller technology enhances reliability and reduces dependency on mechanical locks, minimizing the risk of unauthorized entry. Overall, the system serves as a practical solution for security applications and demonstrates the potential for further improvements, such as remote accessibility and password recovery features, in future iterations.

4. CONCLUSION AND FUTURE WORK

The Password-Based Door Locking Security System effectively enhances security by allowing access only to authorized users through password verification using the AT89S52 microcontroller. It successfully prevents unauthorized entry and provides a simple yet reliable security mechanism. In the future, features such as remote access, password recovery, and biometric authentication can be added to improve functionality and make the system more secure and user-friendly.

REFERENCES

[1] Y. S. R. - et al., “Advanced IoT-Based Smart Home Security System,” Int. J. Sci. Technol., vol. 16, no. 2, p. 4955, May 2025, doi: 10.71097/IJSAT.v16.i2.4955.

[2] J. Dahmen, D. J. Cook, X. Wang, and W. Honglei, “Smart secure homes: a survey of smart home technologies that sense, assess, and respond to security threats,” J. Reliab. Intell. Environ., vol. 3, no. 2, pp. 83–98, Aug. 2017, doi: 10.1007/s40860-017-0035-0.

[3] K. N. Sai, Dr. T. Sunil, and Dr. M. Eshwarappa, “A comprehensive review of door lock security systems,” Int. J. Circuit Comput. Netw., vol. 5, no. 1, pp. 12–17, Jan. 2024, doi: 10.33545/27075923.2024.v5.i1a.61.

[4] Department of Electronics and Communications Engineering, Jawaharlal Nehru Technological University, Anantapur (Andhra Pradesh) India. et al., “Enhanced Security Methods of Door Locking Based Fingerprint,” Int. J. Innov. Technol. Explor. Eng., vol. 9, no. 3, pp. 1173–1178, Jan. 2020, doi: 10.35940/ijitee.B7855.019320.

[5] P. O. Makanjuola, E. S. Shokenu, H. O. Araromi, P. O. Idowu, and J. D. Babatunde, “An Rfid-Based Access Control System Using Electromagnetic Door Lock and an Intruder Alert System,” J. Eng. Res. Rep., pp. 7–17, July 2022, doi: 10.9734/jerr/2022/v22i1117574.

[6] S. Rohokale, P. G. -, S. K. -, S. U. -, and H. S. -, “Design and Development of a Password-Based Door Lock System Using Microcontroller and Electromechanical Solenoid,” Int. J. Multidiscip. Res., vol. 7, no. 3, p. 44813, May 2025, doi: 10.36948/ijfmr.2025.v07i03.44813.

[7] Ms. Mamatha, P. Aakash, N. Sravya, P. Sneha Sree, and V. Shiva Prasad, “Intrusion Detection for Smart Home Alarm Security System,” Int. J. Eng. Technol. Manag. Sci., vol. 9, no. 3, pp. 85–99, 2025, doi: 10.46647/ijetms.2025.v09i03.015.

[8] A. Marinho Da Silva, A. Marinho Da Silva, and Y. Pinheiro Pires, “Prototype for automating the irrigation system using the arduino UNO R3 prototyping board for water control,” Rev. Interdiscip. E MEIO AMBIENTE RIMA, vol. 6, no. 1, p. e235, Apr. 2024, doi: 10.52664/rima.v6.n1.2024.e235.

[9] H.-I. Jun and H.-C. Lee, “A Study on Software algorithm for Processing n-key roll-over at Matrix Keyboard,” J. Softw. Assess. Valuat., vol. 16, no. 1, pp. 89–94, June 2020, doi: 10.29056/jsav.2020.06.10.

[10] V. Goel, R. Varshney, S. Parashar, S. Ali, and P. Singh, “Laser Based Smart Security Apparatus Using Arduino,” Int. J. Res. Appl. Sci. Eng. Technol., vol. 10, no. 3, pp. 1862–1865, Mar. 2022, doi: 10.22214/ijraset.2022.40986.

[11] G. Sasi, “Motion detection using Passive Infrared Sensor using IoT,” J. Phys. Conf. Ser., vol. 1717, no. 1, p. 012067, Jan. 2021, doi: 10.1088/1742-6596/1717/1/012067.

[12] E. O. Amuta et al., “Motion Detection System Using Passive Infrared Technology,” IOP Conf. Ser. Earth Environ. Sci., vol. 1342, no. 1, p. 012001, May 2024, doi: 10.1088/1755-1315/1342/1/012001.

[13] M. I. M. Rozlan, S. B. Kutty, N. A. Sulaiman, N. S. M. Pakhrudin, S. Saaidin, and M. Kassim, “RFID Based Attendance Monitoring System with LED Authentication,” in 2023 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS), Shah Alam, Malaysia: IEEE, June

2023,pp.85–90.doi: 10.1109/I2CACIS57635.2023.10193394.

[14] Dr. A. Gangopadhyay, "Design and Implementation of an IOT Enabled Classified Authentication System using LabVIEW," Int. J. Res. Appl. Sci. Eng. Technol., vol. 11, no. 4, pp. 2170–2174, Apr. 2023, doi: 10.22214/ijraset.2023.50421.