International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 08 | Aug 2026 www.irjet.net p-ISSN: 2395-0072

IoT-Based Keypad Controlled Smart Door Lock System

Design and Implementation of a Password-Based Electronic Access Control System

Saraswathi R Devadiga[1], Jayashri[2], Alsha[3], Fathima Jazeela[4]

[1,2]*Department of BCA, Trisha Vidya College of Commerce and Management, Katpady, Karnataka, India.*

Abstract-*ecurity is an essential requirement in homes, offices, institutions, laboratories, hostels, and other controlled environments. Conventional door locks depend on physical keys, which may be lost, broken, or copied. This paper presents the design and implementation of a keypad-based electronic door locking system using an Arduino UNO microcontroller, matrix keypad, servo motor, and LCD display. The user enters a predefined password through the keypad, and the Arduino verifies the entered value against the password stored in its memory. When authentication is successful, the servo motor moves the locking mechanism to the unlocked position for a short duration and then returns to the locked position automatically. When authentication fails, access is denied and an appropriate message is displayed. The LCD also provides user prompts while concealing the entered password using asterisks. The proposed system is simple, low-cost, and suitable as a prototype for password-based access control. Although the project is described using IoT concepts, the supplied implementation does not include an active remote-access facility; Wi-Fi, Bluetooth, mobile control, biometrics, alarms, and access logging are identified as future enhancements.*

Keywords: Smart door lock, IoT, Arduino UNO, keypad, password authentication, servo motor, LCD, embedded system, access control.

1. INTRODUCTION

Security has become increasingly important in residential, institutional, and workplace environments. Traditional lock-and-key mechanisms remain widely used, but physical keys can be misplaced, damaged, or duplicated without authorization. These limitations have encouraged the development of electronic access-control systems in which authentication is performed through a digital credential.

A keypad-controlled door lock replaces the physical key with a password. In the proposed system, a matrix keypad provides the user interface, while an Arduino UNO processes the entered password. A servo motor performs the physical locking and unlocking operation, and an LCD provides feedback such as access granted, access denied, and password-entry prompts. The supplied project describes the design as an IoT-oriented security system, while also noting that remote access is not present in the current version.

The purpose of this work is to develop a simple, affordable, and user-friendly electronic door lock that demonstrates password authentication, automatic unlocking, and automatic relocking.

2. PROBLEM STATEMENT

Physical keys introduce risks associated with loss, duplication, and unauthorized use. A secure electronic alternative should provide controlled access without requiring a physical key while remaining simple and affordable. The proposed project addresses this problem through password-based authentication using a keypad and a microcontroller-controlled servo locking mechanism.

3. OBJECTIVES

- To design a keypad-based door locking system using password authentication.

- To reduce dependence on physical keys.
- To verify user access through a predefined password stored in the Arduino.
- To automatically unlock the door when the correct password is entered.
- To automatically relock the door after a short predefined period.
- To display clear access and system messages through an LCD.
- To develop a simple, reliable, and affordable prototype that can be extended with IoT features.

4. REQUIREMENT ANALYSIS

Requirement analysis identifies the hardware and software required to implement the proposed system. The supplied project report specifies the following components.

Category	Component	Purpose
Hardware	Arduino UNO	Main controller for processing keypad input and controlling outputs.
Hardware	Matrix keypad	Accepts password input from the user.
Hardware	Servo motor	Provides the physical locking and unlocking mechanism.
Hardware	LCD display	Displays prompts, access granted, access denied, and other messages.
Hardware	Jumper wires	Electrical connections between modules.
Hardware	Power supply	Provides operating power to the system.
Software	Arduino IDE	Used to write, compile, and upload the program.
Software	Embedded C	Programming language used for the controller logic.
Software	Arduino libraries	Support keypad, servo, and LCD communication.

5. SYSTEM ARCHITECTURE

The system can be represented as a sequence of input, processing, display, and actuation stages. The keypad forms the input layer. The Arduino UNO is the processing and decision-making layer. The LCD is the user-feedback layer, and the servo motor is the actuation layer. The password is stored in the controller program and is compared with the value entered by the user.

Stage	Module	Input/Output	Function
Input	Matrix keypad	User password	Collects key presses.
Processing	Arduino UNO	Password string	Compares input with stored password.
Display	LCD	System status	Shows prompts and authentication result.
Actuation	Servo motor	Control signal	Moves the lock between locked and unlocked positions.

6. MODULE DESCRIPTION

6.1 Keypad Module

The keypad is the primary user-input device. It allows the user to enter the password through individual key presses. The controller reads the key sequence and temporarily stores it until the complete password has been entered.

6.2 Control Module – Arduino UNO

The Arduino UNO acts as the central controller. It receives keypad input, compares the entered password with the predefined password stored in memory, controls the servo motor, and updates the LCD display. This provides the decision-making function of the system.

6.3 Display Module – LCD

The LCD provides a simple interface between the system and the user. It displays prompts for password entry and communicates the result of authentication. During password entry, the project uses asterisks instead of displaying the actual characters, providing basic visual privacy.

6.4 Locking Module – Servo Motor

The servo motor provides controlled mechanical movement for the lock. When the password is correct, the Arduino sends a control signal that rotates the servo to the unlocking position. After a short duration, the servo returns to its original position and locks the door.

7. SYSTEM DESIGN AND IMPLEMENTATION

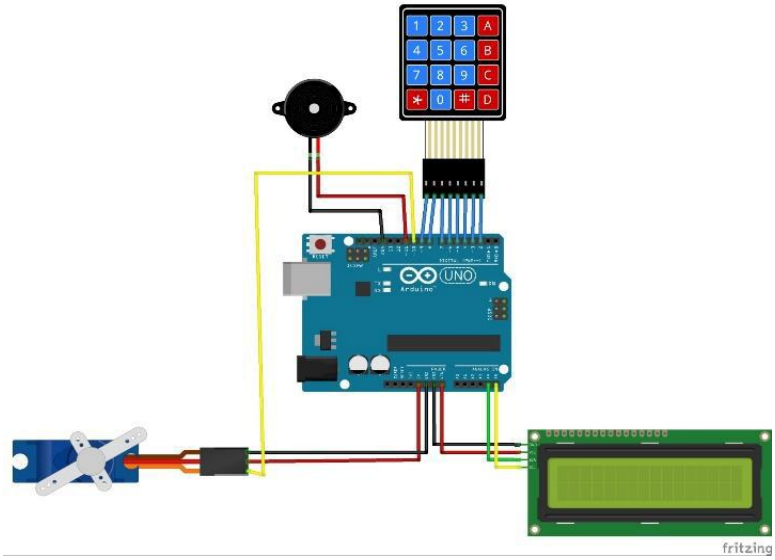
All hardware components are connected to the Arduino UNO. The keypad is connected to digital pins so that the controller can detect user key presses. A fixed password is defined in the program. The user enters the password, and the controller temporarily stores the entered sequence.

The entered password is represented on the LCD using asterisks. Once the password is complete, the Arduino performs a comparison with the stored password. If the two values match, the servo moves to unlock the door. After a few seconds, the servo returns to the original position and the door is automatically locked. If the values do not match, the LCD displays a wrong-password message and the system waits for another attempt.

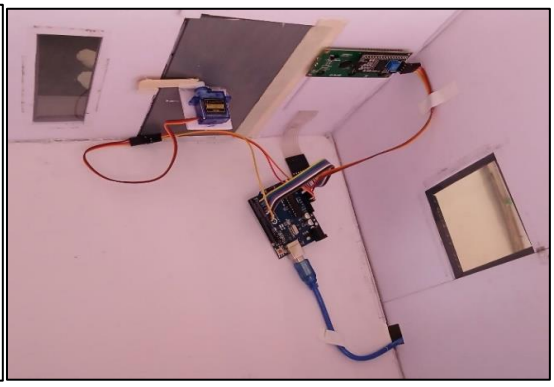
8. WORKING PRINCIPLE

The system begins when power is supplied to the controller and connected modules. The LCD prompts the user to enter a password. Each key press is detected by the Arduino and added to the temporary password input. The LCD masks the entered value using asterisks.

After password entry is complete, the Arduino compares the input with the predefined password. A correct password results in an access-granted condition, causing the servo to unlock the door. The door remains unlocked for a short period and then locks automatically. An incorrect password results in access denial, after which the system resets and waits for the next attempt.



Front View of the Project Model



Internal Hardware Setup of the System

9. CONTROL ALGORITHM

1. Initialize the Arduino, keypad, LCD, and servo motor.
2. Display the password-entry prompt on the LCD.
3. Read each key pressed by the user.
4. Store the entered characters temporarily and display them as asterisks.
5. Detect completion of password entry.
6. Compare the entered password with the predefined stored password.
7. If the password is correct, display an access-granted message and rotate the servo to unlock.
8. Wait for the predefined unlocking duration.
9. Return the servo to the locked position.
10. If the password is incorrect, display an access-denied or wrong-password message.
11. Reset the input and wait for the next authentication attempt.

10. SECURITY CONSIDERATIONS

The system provides basic authentication through a password rather than a physical key. Masking the password on the LCD prevents the entered characters from being directly visible to nearby observers. However, the supplied project identifies

password confidentiality as an important limitation. Since the current design uses a fixed password and does not provide remote access, its security level is appropriate to a prototype rather than a complete enterprise access-control system.
The project report does not describe encryption, user accounts, password recovery, attempt logging, or alarm mechanisms. These functions should therefore not be considered part of the implemented system. They can be incorporated in future versions.

11. APPLICATIONS

- Homes and apartments for basic electronic home security.
- Offices and staff rooms for controlled access.
- Hostels and hotels for restricted-entry applications.
- Laboratories and other restricted areas.
- Storage rooms requiring controlled access.

12. ADVANTAGES

- Eliminates dependence on physical keys.
- Reduces the risk associated with lost or duplicated keys.
- Simple and easy-to-use password-based interface.
- Low-cost prototype design.
- Automatic locking after successful access.
- LCD feedback makes system operation clear to the user.
- Hardware and software can be modified for future upgrades.

13. LIMITATIONS

- Authentication is limited to password-based input.
- The current design uses a fixed password length.
- No remote access facility is implemented in the current system.
- Overall security depends on keeping the password confidential.
- The supplied project does not provide quantitative security or reliability test results.
- The current system does not describe biometric authentication, access logging, or an alarm for repeated failed attempts.

14. TESTING AND EVALUATION

The supplied project report describes the working process and expected behavior but does not provide numerical experimental results. For a formal research evaluation, the following tests can be performed without assuming results that have not been measured.

Test	Procedure	Measurement	Purpose
Correct-password test	Enter the valid password repeatedly.	Successful unlock rate	Verify authentication and actuation.
Incorrect-password test	Enter invalid passwords.	Access-denial rate	Verify rejection of unauthorized input.
Auto-lock test	Observe the lock after successful authentication.	Time to automatic relocking	Verify automatic security behavior.
Input masking test	Observe LCD during password entry.	Visibility of entered password	Verify basic password privacy.
Repeated-use test	Perform multiple authentication cycles.	Number of successful cycles	Assess operational consistency.
Power/restart test	Restart the controller and	System recovery behavior	Verify initialization and

	repeat operation.		repeatability.

15. RESULTS AND DISCUSSION

Based on the supplied project description, the prototype demonstrates the intended sequence of password entry, verification, servo-based unlocking, LCD feedback, and automatic relocking. The design directly addresses the stated objective of replacing a physical key with a password authentication mechanism.

The current project report does not contain measured data such as authentication latency, failure rates, number of repeated cycles, servo positioning accuracy, or comparative security measurements. Accordingly, this paper does not claim numerical performance improvements. A future experimental study should record these parameters and compare the proposed system with a conventional lock or other electronic authentication methods.

16. FUTURE ENHANCEMENTS

The project identifies Wi-Fi or Bluetooth connectivity as a future enhancement for remote access. A mobile application could provide improved user convenience. Biometric authentication, including fingerprint or face recognition, could strengthen authentication. An alarm could be introduced after multiple incorrect password attempts, and an access-monitoring facility could record entry details.

Additional development could combine multiple authentication factors, such as password plus biometric verification, and introduce secure user management and event logging. These features would move the prototype toward a more comprehensive smart security system.

17. CONCLUSION

The IoT-based keypad-controlled smart door lock provides a simple electronic alternative to a traditional key-based locking mechanism. By combining an Arduino UNO, keypad, LCD, and servo motor, the system performs password authentication and controlled physical access. Successful authentication unlocks the door for a short period, after which the system automatically returns to the locked state.

The project demonstrates fundamental concepts of microcontrollers, embedded programming, and IoT-oriented security systems. Its current implementation is a low-cost prototype with limited authentication and no remote access. The proposed future enhancements wireless connectivity, mobile control, biometric authentication, alarms, and access monitoring—provide a clear path toward a more advanced smart security solution.

REFERENCES

[1] Arduino Documentation. Arduino official documentation and development resources.
[2] Arduino Keypad Library. Arduino Playground, Keypad library documentation.
[3] Arduino Servo Library. Arduino reference documentation for servo motor control.
[4] Electronics Hub. IoT and embedded-system learning resources.
[5] CircuitDigest. IoT, Arduino, and embedded-system technical resources.

AUTHOR AND PROJECT INFORMATION

Project Guide: Prof. Saraswati, Assistant Professor, Department of Computer Applications.
Team Members: Jayashri, Alsha, Fathima Jazeela, and Almira.