Vol. 2 - No. 1
September 2024 E-ISSN: 2584-0657

IoT-Based Password-Protected Door Locking System

Dr. S. Usha, S. Ashwin, K. K. Bhargava, K. Chethan
Department of Computer Science Engineering
Rajarajeswari College of Engineering, Bengaluru, Karnataka, India

Abstract
The IoT-based Password-Protected Door Locking System utilizes an Arduino Uno micro controller, a membrane keypad force-cure password input, a servomotor for door actuation, and a stable power supply. This system integrates IoT technology to enhance traditional door security by enabling remote access and control. It operates by receiving and processing password inputs through the keypad, subsequently controlling these rvo motor to unlock the door upon correct password entry. Key features include real-time monitoring and management of the door lock status via an IoT plat- form, allowing for remote accessibility and ensuring heightened security and convenience. This project exemplifies the efficacy of IoT in augmenting home security with enhanced control and reliability.

Keywords
Arduino Uno, IoT, Password Protection, Home Security, Numeric Passcode, Authorisation

I. INTRODUCTION

In an era where technological advancements continually re shape our daily lives, the integration of smart solutions into traditional systems becomes imperative for enhanced security and convenience. The Internet of Things (IoT) has emerged as a pivotal technology, offering innovative ways to connect and control devices remotely. This project introduces an IoT- based Password-Protected Door Locking System, a marriage of traditional door security and cutting-edge IoT technology. The conventional lock and key mechanisms, while effective, a re-evolving to meet the demands of a digitally inter connected world. This project utilizes components suchasan Arduino Uno micro controller, a membrane keypad, a servo motor, and a reliable power supply to transform a standard door into an intelligent and secure access point. The system employs a password-based authentication method, combining the familiarity of key-padentry with the sophistication of IoT connectivity. The Arduino Uno serves as the central processing unit, orchestrating the authentication process and controlling these rvo motor responsible for unlocking the door. The membrane keypad provides a secure means for users to input passwords, making the system accessible to a wide range of individuals. By integrating IoT capabilities, this project enables users to remotely monitor and control the door lock system, adding a layer of convenience and flexibility to traditional security measures. This project not only addresses the need for heightened security but also offers a glimpse into the future of access control, where physical devices seam lessly connect to the digital realm. The following sections will delve into the details of the components, functionalities, and potential applications of this IoT-based Password-Protected Door Locking System, showcasing its potential to redefine the standards of door security in both residential and commercial settings.

II. EXISTING SYSTEM

Traditional door locking systems often lack the versatility and advanced security features demanded by the evolving need sof today's residential and commercial spaces. The reliance on conventional lock and key mechanisms poses limitations in terms of remote access, user-specific access control, and real-time monitoring. Additionally, with the increasing integration of IoT technology into various aspects of daily life, there is a growing need for intelligent, connected solutions that enhance security while providing convenience.
The absence of a robust, IoT-based, password-protected door locking system presents a gap in the market for a solution that seamlessly blends traditional security with modern connectivity. Current systems often over look the integration of IoT capabilities, leaving users with limited options for remote management and monitoring. Furthermore, the need for a secure, user friendly, and customizable authentication method, such as a password-based system, remains unmet in many existing door locking solutions.

To address these challenges, there is a cleard emand for a comprehensive IoT-based Password-Protected Door Locking System that leverages the capabilities of Arduino Uno and other components. This system should provide a secure and efficient means of access control, offering users the flexibility to manage and monitor their doors remotely while maintaining the integrity of a password-based authentication mechanism. Developing such a system will contribute to the advancement of smart security solutions, ensuring a balance between traditional security measures and the capabilities offered by the Internet of Things.

III. PROPOSED SYSTEM

Design and Implement a Secure Password Authentication System

Develop a robust password-based authentication mechanism that ensures secure access control, requiring users to input a predefined password for door unlocking.

Integrate Arduino Uno Micro Controller

Utilize the capabilities of the Arduino Uno microcontroller to serve as the central processing unit, managing the authentication process and controlling the servo motor for door unlocking.

Incorporate Servo Motor for Door Locking Mechanism

Integrate a servo motor into the system to physically control the door locking mechanism. The servo motor should respond to the Arduino Uno's commands based on the successful authentication of the entered password.

Implement IOT Connectivity for Remote Monitoring and Control

Enable Internet of Things (IoT) capabilities to allow users to monitor and control the door locking system remotely. This includes the development of a web or mobile interface for convenient and secure remote access.

Ensure Power Supply Stability

Implement a stable power supply system to ensure continuous and reliable operation of the door locking system, minimizing the risk of unauthorized access due to power disruptions.

Enhance User-Friendliness with Membrane Keypad

Incorporate a membrane keypad as the user interface for entering passwords, ensuring a user-friendly and secure input method.

Implement Security Notifications

Optionally, provide the system with the capability to send notifications or alerts to authorized users in the event of unauthorized access attempts, enhancing overall security.

Evaluate and Optimize System Performance

Conduct thorough testing and evaluation of the system to identify potential vulnerabilities and areas for improvement. Optimize the system for efficiency, reliability, and security.

Explore Future Extensions and Customization

Investigate possibilities for future system extensions, such as biometric authentication or integration with other smart home devices, to enhance the overall functionality and customization options of the IoT-based Password-Protected Door Locking System.

IV. COMPONENTS USED

Arduino Uno

At mega 328 Microcontroller -It is a single chip Microcontroller of the At mel family. The process or code inside it is of 8-bit. It combines Memory (SRAM, EEPROM, and Flash), Analog to Digital Converter, SPI serial ports, I/O lines, registers, timer, external and internal interrupts, and oscillator.

ICSP pin - The In Circuit Serial Programming pin allows the user to program using the firmware of the Arduino board.

Power LED Indicator - The ON status of LED shows the power is activated. When the power is OFF, the LED will not light up.

Digital I/Opins - The digital pins have the value HIGH or LOW. The pins numbered from D0 to D13 are digital pins.

TX and RX LEDs - The successful flow of data is represented by the lighting of these LEDs.

AREF - The Analog Reference (AREF) pin is used to feed a reference voltage to the Arduino UNO board from the external power supply.

Reset button - It is used to add a Reset button to the connection.

USB - It allows the board to connect to the computer. It is essential for the programming of the Arduino UNO board.

Crystal Oscillator-The Crystal oscillator has a frequency of 16 MHz, which makes the Arduino UNO a powerful board.

Voltage Regulator - The voltage regulator converts the input voltage to 5V.

GND - Ground pins. The ground pin acts as a pin with zero voltage.

Vin - It is the input voltage.

Analog Pins - The pins numbered from A0 to A5 are analog pins. The function of Analog pins is to read the analog sensor used in the connection. It can also act as GPIO (General Purpose Input Output) pins.

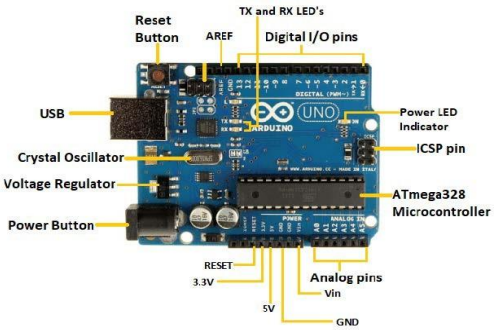

Figure 1: Arduino UNO Board

LCD Display

The term LCD stands for liquid crystal display. It is one kind of electronic display module used in an extensive range of applications like various circuits & devices like mobile phones, calculators, computers, TV sets, etc. These displays are mainly preferred for multi segment light-emitting diodes and seven segments. The main benefits of using this module are in expensive; simply programmable, animations, and there are no limitations for displaying custom characters, special and even animations, etc.

Pin Description

Pin 1 (Ground/Source Pin): This is a GND pin of display, used to connect the GND terminal of the microcontroller unit or power source.

Pin 2 (VCC/Source Pin): This is the voltage supply pin of the display, used to connect the supply pin of the power source.

Pin 3 (V0/VEE/Control Pin): This pin regulates the difference of the display, used to connect a changeable POT that can supply 0 to 5V.

Pin 4 (Register Select/Control Pin): This pin toggles among command or data register, used to connect a microcontroller unit pin and obtains either 0 or 1(0 = data mode, and 1 = command mode).

Pin 5 (Read/Write/Control Pin): This pin toggles the display among the read or writes operation, and it is connected to a microcontroller unit pin to get either 0 or 1 (0 = Write Operation, and 1 = Read Operation).

Pin 6 (Enable/Control Pin): This pin should be held high to execute Read/Write process, and it is connected to the microcontroller unit & constantly held high.

Pins 7-14 (Data Pins): These pins are used to send data to the display. These pins are

connected in two-wire modes like 4-wire mode and 8-wire mode. In 4-wire mode, only four pins are connected to the microcontroller unit like 0 to 3, whereas in 8-wire mode, 8-pins are connected to microcontroller unit like 0 to 7.

Pin 15 (+ve pin of the LED): This pin is connected to +5V

Pin 16 (-ve pin of the LED): This pin is connected to GND.

Figure 2 shows an LCD Panel:

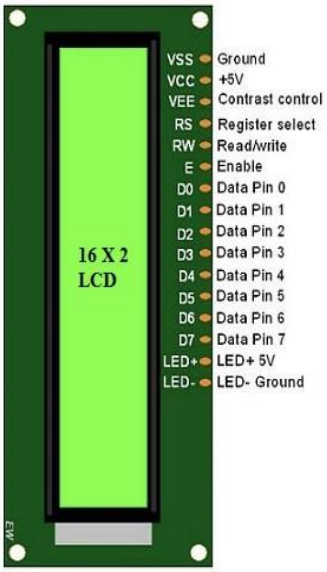

Figure 2 LCD Panel

Power Supply

It is used to provide power to all components. It will take 12 v input voltage and convert it in three voltages of 3.3, 5, 12 volts.

Power supply specification

- Input voltage: 12v
- Output voltage: +3.3v, +5v, +12v
- Maximum load: 0.5 amp
- Frequency: 16MHz

Figure 3 shows a Power Supply:

Figure 3 Power Supply

V. SERVO MOTOR

Servo motors are high torque motors which are commonly used in robotics and several other applications due to the fact that it's easy to control their rotation. Servo motors have a geared output shaft which can be electrically controlled to turn one (1) degree at a time. For the sake of control, unlike normal DC motors, servo motors usually have an additional pin asides the two power pins (Vcc and GND) which is the signal pin. The signal pin is used to control the servo motor, turning its shaft to any desired angle. Servo's have high current requirement so when using more than one servo motor with the Arduino, it is important to connect their power connections to an external power supply as the Arduino may not be able to source the current needed for the servo. Since we will be using just one servo in this tutorial its fine to power it with an Arduino.

Figure 4 shows a Servo Motor

Figure 4 Servo Motor

VI. APPLICATIONS

Residential Security: The IoT-based Password-Protected Door Locking System is well-suited for residential applications, providing homeowners with an intelligent and secure means of controlling access to their homes.

Commercial Spaces: Businesses can deploy this system to enhance the security of office spaces, meeting rooms, or other restricted areas, allowing for customizable access control.

Smart Apartments and Condominiums: The system can be implemented in smart apartment complexes or condominiums to provide residents with secure and remotely manageable door access.

Rental Properties: Landlords and property managers can use the system to manage access to rental properties, allowing for easy and secure keyless entry for tenants.

Remote Monitoring for Vacation Homes: The IoT connectivity feature enables users to remotely monitor and control the door lock, making it ideal for securing vacation homes or properties.

Educational Institutions: The system can be employed in educational institutions to secure class- rooms, laboratories, or administrative offices, with the ability to customize access for different personnel.

Secure Server Rooms: For businesses with server rooms or data centers, the system ensures secure access control, preventing unauthorized entry to critical infrastructure.

Healthcare Facilities: In healthcare settings, the system can be used to control access to sensitive areas, such as medication storage rooms or patient records.

Integration with Smart Cities: In the context of smart city initiatives, the system can contribute to intelligent access control solutions for public spaces or government buildings.

Temporary Access Control: The system can be utilized for events or situations where temporary ac- cess control is needed, offering a flexible and customizable solution.

Retail Stores: Retailers can use the system to secure backrooms or storage areas, ensuring that only authorized personnel can access these spaces.

Airbnb and Short-Term Rentals: The system provides a convenient and secure solution for managing access to Airbnb or other short-term rental properties, enhancing the overall guest experience.

VII. CONCLUSION

In conclusion, the IoT-based Password-Protected Door Locking System represents a significant advance- ment in access control technology, combining the reliability of a password-based authentication system with the versatility of IoT connectivity. This project successfully integrates an Arduino Uno microcontroller, a membrane keypad, a servo motor, and a stable power supply to create a secure and remotely manageable door locking mechanism. The system addresses the limitations of traditional lock and key methods by providing enhanced security features, user-friendly interaction, and the flexibility of remote monitoring and control through IoT. The advantages of this system include its robust security measures, user friendly interface, and potential for customization in various applications such as residential security, commercial spaces, and temporary access control scenarios. The integration of real-time notifications and the possibility of future extensions, like biometric authentication, add further layers of sophistication to the system. However, it is crucial to acknowledge the potential challenges, such as dependency on a stable power supply and the need for ongoing maintenance. These considerations highlight the importance of careful implementation and user education to maximize the system's effectiveness. In essence, the IoT-based Password-Protected Door Locking System bridges the gap between traditional security measures and the demands of a connected world. Its successful implementation holds promise for reshaping access control systems, contributing to the evolution of secure and intelligent solutions in both residential and commercial settings.

VIII. REFERENCES

[1] K. Bhat, and S. P. Kini, "Password Enabled Door Locking System using Arduino and IoT," *International Journal of Engineering Research & Technology*, vol. 6, 2018.

[2] K. Gupta, N. Jiwani, M. H. Uddin Sharif, M. A. Mohammed, and N. Afreen, "Smart Door Locking System Using IoT," *International Conference on Advances in Computing, Communication and Materials (ICACCM)*, 2022.