UTTARA UNIVERSITY

Department of Electrical & Electronics Engineering

Project On

‘‘Password based circuit Breaker’’

In Partial fulfilled requirements for the B.Sc Degree of Electrical & Electronics Engineering

Author’s Name	ID
MD. NAHID HASAN	2213171050
MD. RONY AKTAR	2213171067
RASEL UDDIN	2213171068

This book is for the partial fulfilment of B.Sc in Electrical and Electronic Engineering from Uttara University

Date of Submission: December- 2024

DECLARATION

This project, titled **"Password Based Circuit Breaker,"** represents original work conducted independently in the laboratories of the Department of Electrical and Electronic Engineering at **Uttara University**. It is submitted in partial fulfillment of the requirements for the Bachelor of Science degree in Electrical and Electronic Engineering.

This work has not been previously submitted, in whole or in part, for any other degree, diploma, or qualification at this or any other institution. I have taken necessary steps to identify potential risks associated with this research, and all required ethical and safety approvals have been obtained where applicable. I take full responsibility for the content and originality of this work and certify the accuracy and reliability of the information presented herein.

Signature of the Supervisor

Zakir Hossain

senior lecturer

Department of Electrical and ElectronicEngineering

Uttara University

Signature of the Author's

Name	ID	Signature
MD. NAHID HASAN	2213171050	
MD. RONY AKTAR	2213171067	
RASEL UDDIN	2213171068	

APPROVAL

The project entitled **"Password Based Circuit Breaker"** submitted by MD. Nahid Hasan **ID:** 2213171050**,** MD. Rony Aktar **ID:** 2213171067**,** Rasel Uddin **ID:** 2213171068 has been done under my supervision and accepted as adequate in partial fulfillment of the requirements for the degree of **Bachelor of Science in Electrical and Electronic Engineering** in **February, 2025.**

_____

Zakir Hossain

senior lecturer

Department of Electrical and Electronic Engineering
Uttara University

ACKNOWLEDGEMENT

First and foremost, we would like to express our heartfelt gratitude to Almighty Allah for His guidance and support throughout the completion of this final-year project.

We are profoundly thankful to **Zakir Hossain**, senior Lecturer in the Department of Electrical and Electronic Engineering at Uttara University. His extensive knowledge and dedication to the field of **"Password Based Circuit Breaker"** greatly enriched our work. His patience, insightful feedback, and continuous encouragement were invaluable to the success of our project. We also wish to acknowledge our classmates for their collaborative spirit and engaging discussions, which deepened our understanding and contributed significantly to this project. Finally, we extend our deepest appreciation to our parents for their unwavering support and encouragement throughout our academic journey. Their belief in us has been a constant source of motivation.

On behalf of

MD. Nahid Hasan

ID: 2213171050

MD. RONY AKTAR

ID: 2213171067

RASEL UDDIN

ID:2213171068

ABSTRACT

The "Password Based Circuit Breaker" project addresses critical safety and security challenges in managing electrical systems. This innovative solution employs a password-controlled mechanism to regulate access to electrical loads, ensuring that only authorized personnel can activate or deactivate the circuit breaker. Utilizing an Arduino Nano microcontroller, the system integrates a keypad for password input, an LCD display for real-time feedback, and a relay for controlling the electrical load. When the correct password is entered, the relay is activated, allowing or disallowing the connection to the electrical load, while incorrect entries trigger an alert through a buzzer. This project not only enhances operational safety but also mitigates the risk of unauthorized access, particularly in high-stakes environments such as industrial settings. The design includes a backup battery to ensure continuous operation during power outages and a booster circuit for stable voltage levels. By integrating digital control with traditional electrical components, this project exemplifies a secure and user-friendly approach to managing electrical systems, paving the way for safer applications in both residential and industrial contexts. Ultimately, the "Password Based Circuit Breaker" contributes to reducing electrical accidents and enhancing the reliability of electrical infrastructure.

Table of Content's

CHAPTER ONE
INTRODUCTION

1.1 Introduction

In an era where electrical systems are integral to daily life, ensuring their safety and security has become paramount. The proliferation of electrical devices in residential, commercial, and industrial environments has heightened the risk of unauthorized access and control. Traditional circuit breakers, while essential for protecting electrical circuits from overloads and faults, often lack robust security features. This vulnerability can lead to severe consequences, including equipment damage, electrical hazards, and potential loss of life.

In this project seeks to address these critical issues by integrating a password-controlled mechanism into the operation of electrical loads. At the heart of this innovative system is the Arduino Nano microcontroller, which serves as the control unit for managing user inputs and the functionality of connected devices. By employing a keypad for password entry, this system ensures that only authorized users can activate or deactivate electrical loads, significantly reducing the risk of accidental or malicious interference. The need for enhanced security in electrical systems is underscored by increasing incidents of unauthorized access, particularly in environments where multiple users have access to electrical controls. For instance, in industrial settings, where heavy machinery operates, unauthorized manipulation can lead to catastrophic failures or safety breaches. Similarly, in residential applications, the ability to control electrical loads securely can prevent accidents and ensure that only designated individuals have the authority to manage power supply. Additionally, the system's user-friendly interface, facilitated by an LCD display, allows for clear communication with users regarding system status, password prompts, and feedback on access attempts. This feature not only enhances user experience but also promotes awareness and accountability in electrical management. Furthermore, the incorporation of safety measures such as alert mechanisms via a buzzer for incorrect password entries reinforces the security framework of the system. It serves as an immediate notification to users, enabling timely responses to potential breaches. This project not only represents a significant advancement in the realm of electrical safety but also sets the foundation for future innovations in automated control systems. By merging digital control technologies with traditional electrical components, this initiative aims to pave the way for safer, more efficient, and secure electrical systems across various applications.[1]

1.2 Problem Statement

The project addresses significant challenges related to the security and management of electrical systems. Circuit breakers are essential for maintaining the safety and reliability of electrical systems; however, their traditional designs often lack adequate security features to prevent unauthorized access. The increasing complexity of electrical systems in residential and industrial environments has exposed vulnerabilities. Malfunctions in circuit breakers can lead to outages and create insecure operating conditions, which are further exacerbated during maintenance. In many instances, maintenance personnel must entirely disconnect power lines to ensure safety, causing significant inconvenience to consumers. Moreover, poor communication between maintenance staff and substation operators can increase the risk of accidents, jeopardizing the safety of line workers. Currently, if maintenance work is required on a distribution line, the entire line must be shut down, disrupting service to customers and potentially compromising safety. The reliance on manual control for activating or deactivating the line increases the risk of human error and unauthorized manipulation. Without a secure authentication mechanism, there is no way to ensure that only authorized personnel can operate the circuit breaker. This integrates a microcontroller, relay driver IC, keypad, and LCD display to restrict access to authorized users. This system enhances safety through real-time communication and alerts, ensuring that maintenance can be conducted without compromising system integrity or user safety. By addressing these critical challenges, the project aims to establish a more reliable, secure, and efficient method of managing electrical systems.[7]

1.3 Objective

This project is designed with specific goals that aim to address the challenges associated with the security and management of electrical systems. The primary objectives of this project are as follows:

- Develop a password-controlled system to ensure only authorized users can activate or deactivate electrical loads, enhancing security.
- Implement a keypad and LCD display for intuitive password entry and system feedback.
- Integrate alert mechanisms to notify users of unauthorized access attempts through incorrect password entries.
- Use a booster circuit to maintain stable voltage levels for efficient and reliable operation.
- Include a backup battery to ensure functionality during power outages.

1.4 Methodology

The methodology for developing the **'Password Based Circuit Breaker'** is structured into several comprehensive phases to ensure a robust and effective system. Initially, a detailed plan is formulated, outlining the project requirements, objectives, and the necessary components, including the Arduino Nano, relay module, 4x4 keypad, 16x2 LCD display, and other supporting circuitry. In the hardware setup phase, the components are assembled on a breadboard to facilitate easy connections and modifications. The Arduino Nano serves as the microcontroller, with the relay module connected to control the electrical loads. The relay driver IC is used to interface the relay with the microcontroller, ensuring efficient operation. The keypad is wired to the Arduino Nano to enable user input for password entry, while the LCD display is connected to provide real-time feedback on system status, password prompts, and error messages.

The software development phase involves programming the Arduino Nano using the Arduino IDE. This includes writing code to initialize the keypad and LCD display, read inputs from the keypad, and display messages on the LCD. A password verification system is implemented, where the entered password is compared with a predefined value stored in the microcontroller's memory. Upon a correct password entry, the system activates or deactivates the relay, allowing or interrupting the flow of electricity. If an incorrect password is entered, an error message is displayed, and an alert mechanism, such as a buzzer, is activated to indicate unauthorized access attempts.

Testing is a critical phase of the methodology, where the entire system is rigorously evaluated to ensure functionality and reliability. This includes verifying the response of the relay to password inputs and confirming that the LCD displays the correct messages. Various scenarios are simulated, including correct and incorrect password entries, to assess the system's resilience and responsiveness. Finally, the completed circuit is housed in a protective enclosure that not only safeguards the components but also provides a user-friendly interface for easy interaction with the system. This comprehensive methodology ensures that is effectively designed, implemented, and tested, addressing the challenges associated with electrical system security and management.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The growing demand for safety and efficiency in electrical systems has highlighted limitations in traditional circuit breakers, particularly their lack of security features to prevent unauthorized access. These vulnerabilities can lead to safety risks and inefficiencies in electrical management. This project addresses these challenges by integrating a password-controlled mechanism to restrict access to electrical loads. Leveraging microcontroller-based systems, such as Arduino, enables advanced control, user authentication, and real-time feedback. By incorporating user-friendly interfaces like keypads and LCD displays, this approach ensures intuitive interaction and secure management of electrical systems. This literature review explores existing technologies, including circuit breakers and password-based systems, identifying gaps in traditional methods. It emphasizes the need for secure, efficient solutions and sets the groundwork for the project's innovative contributions.[11]

2.2 Related Research

Recent research highlights several innovative systems for enhancing electrical load management and security. The Password-Based Electrical Load Control System ensures only authorized access to devices, while the Smart Circuit Breaker with Remote Monitoring offers real-time system oversight. Additionally, IoT-Based Smart Electrical Systems with User Authentication leverage advanced connectivity for secure control, and Secure Access Control for Smart Home Systems focuses on safeguarding residential environments through robust authentication methods.

2.2.1 Password-Based Electrical Load Control System

A study by Kumar and Sharma (2020) presented a password-based electrical load control system that enhances the security of home appliances. The researchers implemented an Arduino-based system that requires users to enter a password via a keypad to control electrical devices. This project demonstrated that integrating password protection significantly reduces the risk of unauthorized access to electrical loads. The findings highlighted that the system not only improves safety but also allows users to monitor power usage effectively. The researchers concluded that such systems are crucial for modern smart homes, where security and energy

management are paramount［1］.

2.2.2 Smart Circuit Breaker with Remote Monitoring

Patel et al. (2022) introduced a smart circuit breaker that integrates remote monitoring capabilities to enhance electrical safety. This system utilizes Wi-Fi connectivity to allow users to monitor the status of electrical loads through a mobile application. The researchers emphasized the importance of authentication methods, such as password protection, to prevent unauthorized access to the system. The findings indicated that implementing a smart circuit breaker with remote access not only improves user control but also reduces the likelihood of electrical hazards by enabling timely interventions during fault conditions.[2]

2.2.3 IoT-Based Smart Electrical System with User Authentication

A study by Ali and Khan (2021) explored the integration of IoT technology in smart electrical systems, focusing on user authentication for enhanced security. The researchers designed a system that requires user authentication via passwords and biometrics to access and control electrical loads. This innovative approach ensures that only authorized users can manage electrical devices, mitigating risks associated with unauthorized access. The research demonstrated that combining IoT with strong authentication mechanisms significantly increases the safety and reliability of electrical systems, paving the way for advanced applications in smart grids.[3]

2.2.4 Secure Access Control for Smart Home Systems

In a study conducted by Verma et al. (2021), researchers developed a secure access control mechanism for smart home systems, focusing on password authentication to manage electrical devices. The system integrates various sensors and microcontrollers to provide users with the ability to control home appliances securely. The authors highlighted that using a password-based approach significantly reduces the risk of unauthorized access and potential safety hazards. Their findings suggest that implementing such secure access controls in smart homes not only enhances security but also fosters user trust in automated systems. This research underscores the importance of robust authentication methods in managing electrical loads and ensuring safe operation within residential environments.[4]

2.3 Security Measures in Electrical Systems

In the contemporary landscape of electrical engineering, the importance of security measures in electrical systems cannot be overstated. As electrical systems become increasingly complex and interconnected, they present numerous vulnerabilities that can be exploited if not adequately

protected. This section discusses various security measures implemented in electrical systems, emphasizing their significance in enhancing safety and reliability.

2.3.1 Importance of Security in Electrical Systems

The rising frequency of electrical system failures and incidents of unauthorized access has highlighted the necessity for robust security measures. In both residential and industrial contexts, compromised electrical systems can lead to severe consequences, including equipment damage, financial losses, and, in extreme cases, injuries or fatalities. Security measures are essential to prevent unauthorized access and manipulation of electrical loads, ensuring operational integrity and protecting against potential hazards.[9,10]

2.3.2 Types of Security Measures

Electrical systems utilize various security measures to mitigate risks associated with unauthorized access and operational failures. These measures can be broadly categorized into the following:

1. **Physical Security**: This includes barriers such as fences, locks, and surveillance systems that deter unauthorized physical access to electrical infrastructure. Physical security is fundamental in safeguarding critical components of the electrical grid, including substations and control rooms.
2. **Access Control**: Implementing access control systems, such as keycard entry or biometric authentication, ensures that only authorized personnel can access critical electrical equipment. These systems can be combined with password protection to enhance security further.
3. **Digital Authentication**: The integration of digital security measures, including password-based access controls, plays a crucial role in preventing unauthorized access to electrical systems. Passwords serve as a first line of defense, enabling user authentication before granting access to control functionalities.

2.3.3 Challenges in Implementing Security Measures

Despite the availability of various security measures, several challenges hinder their effective implementation in electrical systems:

1. **Complexity of Systems**: The increasing complexity of electrical systems makes it challenging to identify all potential vulnerabilities. Comprehensive risk assessments are required to ensure that all aspects of the system are secure.
2. **Human Factor**: User-related issues, such as weak passwords or failure to follow security protocols, can compromise even the most sophisticated security systems.

Continuous training and awareness programs are necessary to mitigate these risks.

3. **Cost and Resources**: Implementing comprehensive security measures can be resource-intensive, and budget constraints may limit the extent of security enhancements. Organizations must balance security investments with operational costs.

2.4 Password-Based Systems

Password-based systems have emerged as a fundamental component of security frameworks across various domains, particularly in managing access to electronic and electrical systems. This section explores the significance, functionality, and applications of password-based systems, emphasizing their role in enhancing security and user authentication. [8]

2.4.1 Significance of Password-Based Systems

Password-based systems are crucial for enhancing security in various applications, particularly in managing electrical systems. These systems serve as a first line of defense against unauthorized access, ensuring that only individuals with the correct credentials can operate sensitive equipment. In the context of electrical management, implementing password protection helps prevent accidental or malicious manipulation of circuit breakers and electrical loads, which can lead to safety hazards, equipment damage, and service disruptions. The significance of these systems is further underscored by the increasing complexity of electrical infrastructures, which require robust security measures to safeguard against unauthorized interference. By employing password-based access control, organizations can enhance operational safety, promote accountability, and mitigate risks associated with unauthorized access to electrical systems.

2.4.2 Design and Implementation of Password-Based Systems

The design and implementation of password-based systems involve a systematic approach that combines hardware and software components to create an effective security mechanism. In the case of the **"Password Based Circuit Breaker,"** the system utilizes an Arduino Nano as the microcontroller, which manages user inputs from a keypad and provides feedback through an LCD display. The implementation includes coding the microcontroller to validate the entered password against a stored value, activating a relay to control the electrical load only upon successful authentication. The system may also incorporate alert mechanisms, such as buzzers, to notify users of unauthorized access attempts. Key considerations during the design phase include user interface simplicity, reliability, and responsiveness to ensure that the system is user-friendly and efficient in real-world applications.

2.4.3 Applications of Password-Based Systems in Electrical Management

Password-based systems have a wide range of applications in electrical management, particularly

in enhancing the safety and reliability of electrical infrastructure. These systems can be integrated into various components such as circuit breakers, power distribution units, and smart meters, allowing for secure access control and operation. For instance, in industrial settings, password-based systems can prevent unauthorized personnel from turning on or off machinery, thus ensuring safe operation and reducing the risk of accidents. Additionally, these systems can facilitate remote monitoring and management of electrical loads, where authorized users can access and control equipment from a distance using secure credentials. The integration of password protection not only fortifies security but also promotes efficient energy management by enabling designated personnel to optimize power usage based on operational needs, ultimately contributing to improved safety and efficiency in electrical systems.

2.5 Circuit Breaker Technologies

The evolution of circuit breaker technologies reflects the growing demands for safety, reliability, and efficiency in electrical systems. Traditional circuit breakers have played a critical role in protecting electrical circuits by interrupting the flow of electricity during overload or fault conditions. However, these conventional devices often lack advanced features, limiting their effectiveness in modern applications where real-time monitoring and control are essential.

2.5.1 Evolution of Circuit Breakers

Traditional circuit breakers, such as fuse-based systems and electromechanical breakers, provided basic overcurrent protection but often required manual resetting after tripping. Their limitations include slow response times to electrical faults and inadequate means for communication about system status. As electrical systems have become more complex, the need for circuit breakers that can adapt and respond dynamically to varying load conditions has become apparent.

2.5.2 Modern Innovations in Circuit Breaker Design

Modern circuit breaker designs have introduced automation and smart features that significantly enhance their functionality. Innovations such as digital trip units, remote connectivity, and programmable settings allow for greater customization and integration into smart grid systems. These advancements facilitate better load management, predictive maintenance, and improved energy efficiency, ultimately leading to reduced downtime and enhanced safety in electrical installations.

2.5.3 Role of Microcontrollers in Circuit Breakers

Microcontrollers play a pivotal role in modern circuit breakers by enabling intelligent control and monitoring capabilities. They process data from various sensors and inputs, allowing for real-

time analysis of electrical conditions. This integration not only enhances fault detection and response times but also supports features like remote operation and data logging, which are crucial for effective management of electrical systems. By leveraging microcontrollers, circuit breakers can communicate with other devices, contributing to the development of smart electrical infrastructures.

2.6 Research gap

Previous research on circuit breakers has primarily focused on improving their reliability in protecting electrical systems from overloads and short circuits. However, traditional circuit breakers often lack integrated security features, such as password protection, to prevent unauthorized access. While some studies have explored the use of microcontroller-based systems to enhance automation and control, there is a gap in integrating secure authentication mechanisms with circuit breaker systems, particularly in residential and industrial applications.

This project addresses this gap by introducing a password-controlled access system. By combining microcontroller-based control with user authentication via a keypad and LCD display, the project enhances security, user accountability, and operational transparency. The benefit of this project is its ability to prevent unauthorized manipulation of electrical loads, reducing the risk of accidents and ensuring safer, more reliable electrical system management. Additionally, it introduces a practical solution for real-time user interaction and feedback, addressing the need for secure and efficient electrical load control.[5]

CHAPTER THREE

DESIGN AND DEVELOPMENT

3.1 Introduction

The design and development of this project focus on creating a secure and efficient system for managing electrical loads using a password-protected access control. This chapter provides an in-depth overview of the system's technical framework, design approach, and development process, focusing on key components such as the Arduino Nano microcontroller, LCD display, keypad, relay, and supporting hardware. The primary aim of the system is to address critical security needs in electrical environments, mitigating risks of unauthorized access and reducing potential hazards or operational interruptions. The system's architecture prioritizes both reliability and security, integrating various hardware components to deliver a responsive and robust control mechanism. At the core of this setup, the Arduino Nano microcontroller acts as the control unit, processing user inputs from the keypad and providing feedback via the LCD display. Upon correct password entry, the Arduino Nano signals the relay, which activates or deactivates the connected AC load to safely control power flow. In the event of an incorrect password, an audible alert from a buzzer notifies users of unauthorized attempts, adding an extra layer of security. To ensure stable and continuous operation, a booster circuit and backup battery maintain reliable power during fluctuations or outages. This chapter also explores the software aspects of the project, outlining the programming logic developed to handle password verification, user interaction, and precise control commands. Each stage, from hardware assembly to software coding and rigorous system testing, has been conducted to ensure a seamless user interface and dependable functionality. The objective is to deliver a secure, user-friendly system that enhances safety and control in electrical load management across residential, commercial, and industrial settings.

Finally, the chapter concludes with an overview of the testing process and outcomes. Extensive testing simulated real-world conditions, including correct and incorrect password entries, power fluctuations, and load variations, to validate the system's resilience and reliability. The combined functions of the relay, booster circuit, and backup battery demonstrated the circuit breaker's

ability to maintain functionality during power instability, supporting its practical application as a scalable solution. Through a design that emphasizes security and stability, this project is advances safe and controlled electrical system management. [14,15]

3.2.1 Designed Model block diagram

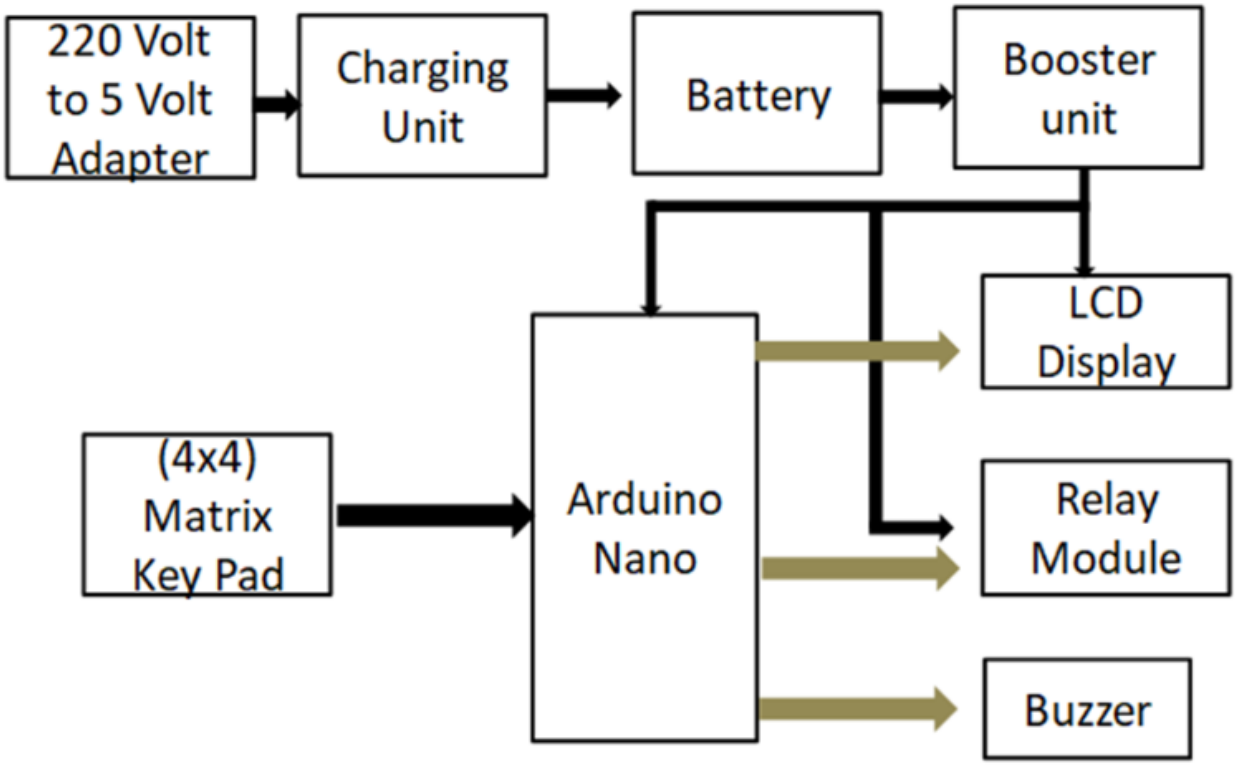

Figure 3.1: Designed model block diagram

The block diagram (Figure 3.1) represents the overall structure and flow of the Password-Based Circuit Breaker system. It shows how the key components interact to achieve secure control over electrical loads. The Arduino Nano acts as the central unit, receiving input from the keypad (for password entry) and processing it. Upon receiving the correct password, the Arduino controls the relay module to turn the AC load on or off. The LCD display provides real-time feedback to the user, indicating system status and authentication results. The buzzer alerts users in case of incorrect password entries, enhancing security. This integrated approach ensures that only authorized users can control the electrical load, enhancing both safety and user interaction.[13]

3.2.2 Circuit Diagram

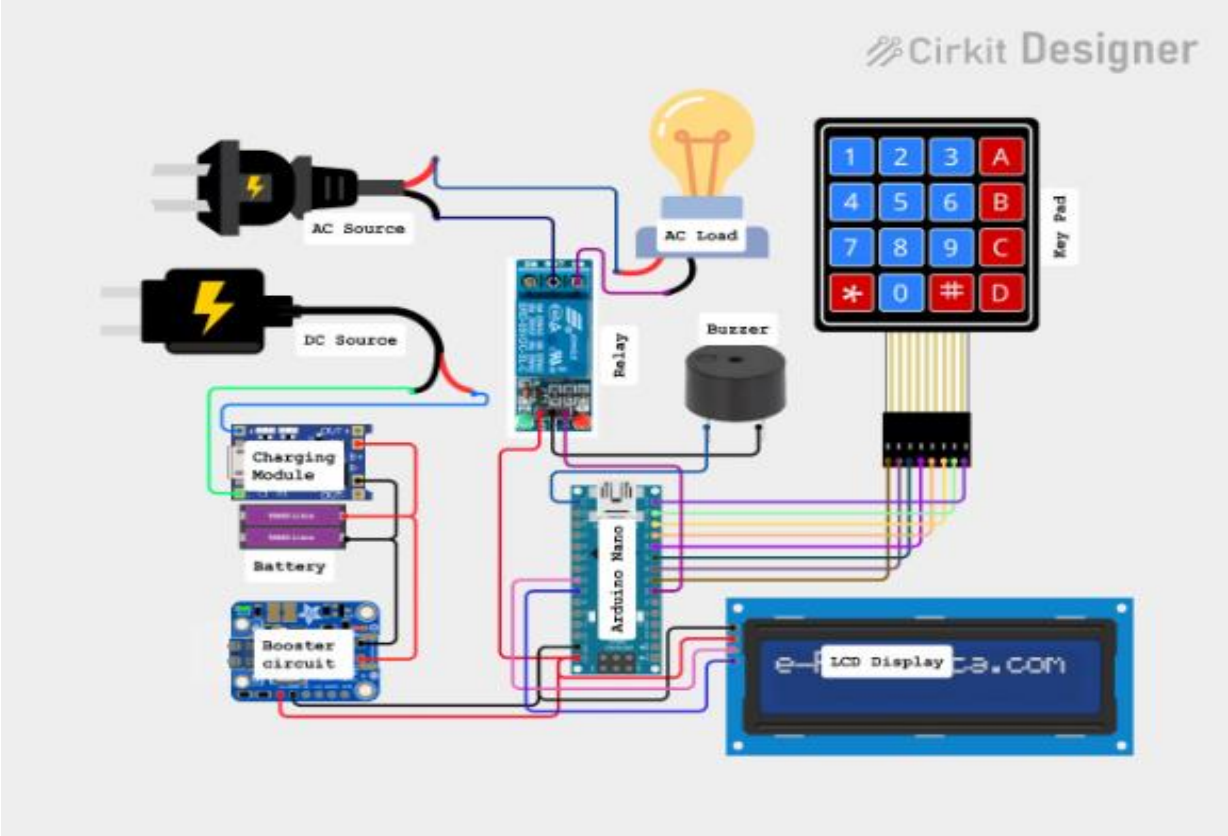

Figure 3.2: Designed model circuit diagram

This diagram represents a **"Password-Based Circuit Breaker"** system using an Arduino Nano as the main controller ***(Fig-3.2)***. The system is designed to improve the security of electrical load management by allowing only authorized users to control the power supply through a password-protected mechanism. The **Arduino Nano** is connected to a power supply system that includes a charging module, battery, and booster circuit, which provides a stable power source and ensures continuous operation during outages.

Key components, such as a 4x4 keypad, relay, LCD display, and buzzer, are integrated into the circuit to facilitate user interaction and feedback. The user enters a password on the keypad, which the Arduino processes to verify authorization. If the correct password is entered, the relay is activated, allowing power to flow to the connected load (such as an AC load). The LCD provides visual feedback, while the buzzer acts as an alert mechanism for incorrect entries, enhancing security. This automated setup offers a reliable solution for secure power control,

suitable for both residential and industrial applications. [2,4]

3.2.3 List of the components

- Arduino Nano
- LCD Display
- Project board
- 220v to 5-volt adaptor
- Relay module
- Ac Source
- Dc source
- Buzzer
- Booster circuit
- Battery
- Key pad
- Jumper wire
- Connecting wire

3.3 Arduino Nano

The Arduino Nano, shown in Fig. 3.3, is a compact microcontroller board powered by the ATmega328P, providing a robust yet space-efficient solution for embedded systems and breadboard applications. Designed to offer the core functionality of larger Arduino boards, the Nano is particularly well-suited for projects requiring a minimal footprint. Operating at 5V with an input voltage range of 7-12V, it can connect to various power sources via the Mini-B USB port for easy programming and power. The board includes 22 digital I/O pins, 6 of which are capable of Pulse Width Modulation (PWM), enabling versatile control over connected devices like LEDs, motors, and other actuators. Additionally, 8 analog input pins make it suitable for monitoring sensors and other analog inputs, providing an adaptable interface for a variety of real-world applications.

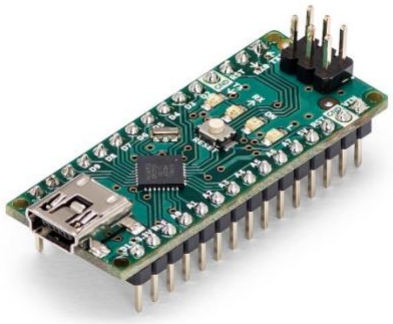

Figure 3.3: Arduino uno

Fig. 3.3 illustrates the Arduino Nano's compact design, which also includes 32 KB of flash memory (with 2 KB allocated for the bootloader), 2 KB of SRAM, and 1 KB of EEPROM. With a 16 MHz clock speed, the Nano delivers reliable processing power for time-sensitive tasks, ensuring smooth control and interaction with peripherals. Unlike some larger Arduino boards, it lacks a dedicated DC power jack, but its size and functionality make it ideal for portable or space-constrained applications. Its open-source architecture and extensive community support further add to its appeal, making the Arduino Nano a popular choice for projects that demand reliability in a small form factor.

SPECIFICATIONS:

Operative Voltage: 5V (5V model) or 3.3V (3.3V model)

Input Voltage: 7-12V for both models (recommended range)

Digital I/O Pins: 14 Pins (6 with PWM capability)

Analog Input Pins: 8 Pins

DC Current per I/O Pin: 40 mA

Flash Memory: 32 kB (2 KB is taken by bootloader)

SRAM: 2 Kbytes

EEPROM: 2 Kbytes

Clock Speed: 16 MHz (5V model) and 8 MHz (3.3V model)

Table 3.1: ARDUINO NANO Configuration

Pin Group	Pin Name	Description
POWER SOURCE	Vin, 5V, 3.3V, GND	-Vin: Input voltage (7-12V) from an external source - 5V: Regulated 5V output to power the board and connected components - GND: Ground pins
Communication INTERFACE	UART(Serial0-erial3), I2C (SCL, SDA), SPI (MOSI, MISO, SCK)	-UART: One serial port (TX/RX) for communication -SPI**:** SPI communication pins (MOSI, MISO, SCK)

		- I2C: I2C protocol pins (SCL, SDA)
INPUT-OUTPUT PINS	D0 to D13	14 digital I/O pins, 6 of which support PWM output.
ANALOG INPUT PINS	A0 to A7	8 analog input pins with 10-bit resolution.
PWM	D3, D5, D6, D9, D10, D11	6 PWM pins providing 8-bit resolution.
RESET	RESET	Resets the controller.
EXTERNAL INTERRUPTS	D2, D3	Pins D2 and D3 provide hardware interrupt functionality.
ANALOG COMPARATOR	AIN0, AIN1	Internal analog comparator with input pins AIN0 and AIN1.

The Table 3.1 provides the accurate configuration details for the Arduino Nano, outlining its power source, communication protocols, digital and analog input/output capabilities, PWM outputs, reset function, external interrupts, and analog comparator feature.

3.4 Liquid Crystal Display (LCD) 16*2

The 16x2 Liquid Crystal Display (LCD), shown in Figure 3.4, is a popular component in Arduino and microcontroller projects, known for its ability to display data in a compact format. This LCD can show 16 characters per line across two lines, making it an ideal replacement for LEDs in many applications. The standard interface for these LCDs is based on the HD44780U controller chip, which facilitates communication between the microcontroller and the display.

The HD44780U controller allows the LCD to operate in either a 4-bit or 8-bit data mode. In 4-bit mode, the display requires a total of seven lines (three control and four data lines), while in 8-bit mode, it requires eleven lines (three control and eight data lines). This flexibility enables users to connect the LCD easily to a variety of microcontrollers.

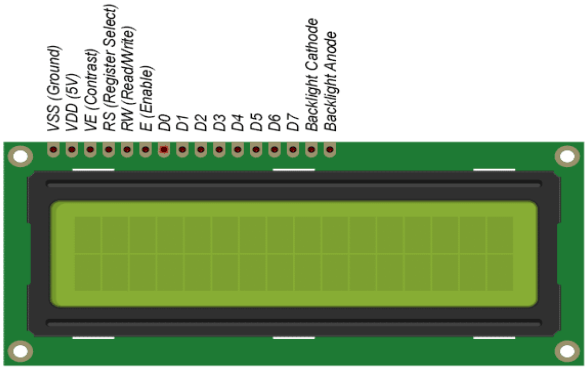

Figure 3.4: LCD 16*2

Features

- The presentation information RAM
- Character initiator ROM
- 160 different 57-dot matrix character patterns
- The display includes internal RAM for data storage and character generation ROM
- It supports 160 different 5x7 dot matrix character patterns
- Microcontrollers can access both display data RAM and character generator RAM
- The LCD offers various functions such as cursor positioning, display on/off, and character blinking.
- It features an i ntegrated circuit that initializes automatically upon power-on

Table 3.2: Pin symbol description

PIN	Sign	Function
1	VSS	GND
2	VDD	+5V
3	V0	Contrast Adjustment
4	RS	H/L Register select signal
5	R/W	H/L Read/write signal
6	E	H/L Enable signal
7	DB0	H/L Data bus line
8	DB1	H/L Data bus line
9	DB2	H/L Data bus line
10	DB3	H/L Data bus line
11	DB4	H/L Data bus line
12	DB5	H/L Data bus line
13	DB6	H/L Data bus line
14	DB7	H/L Data bus line
15	A	+4.2V for LED
16	K	Power supply for BKL (0V)

Table 3.2 shows the pin functions of a 16x2 LCD display. Pins 1 and 2 are for power (VSS for ground and VDD for +5V), while Pin 3 controls the contrast. Pins 4 to 6 manage the register

selection, read/write control, and enable signals, and Pins 7 to 14 form the data bus lines. Pins 15 and 16 provide power for the LCD backlight.

3.5 Booster Circuit

A booster circuit, or DC-DC boost converter, is essential for increasing a lower input voltage to a higher, stable output. In the Password-Based Circuit Breaker, the booster circuit ensures reliable power to components like the Arduino, LCD, and relay, even if input voltage fluctuates. This is achieved through an inductor, switch, diode, and capacitor that work together to boost and smooth the voltage. By providing a consistent power supply, the booster circuit enhances the

system's reliability and supports uninterrupted control over electrical loads.

Figure3.5 Booster Circuit

3.6 Single Channel Relay Module

A relay is an electrically operated switch that allows low-current signals to control high-current circuits. It is commonly used in automatic control systems to manage high-voltage loads, such as motors, lamps, and AC devices, using a minimal input power signal (typically 0 to 5V). The relay provides electrical isolation between the control and load circuits, enhancing safety by preventing damage to low-power components. In the Password-Based Circuit Breaker project, the relay is crucial for controlling the AC load: when the correct password is entered, the microcontroller activates the relay to allow electrical flow, whereas incorrect password attempts

keep the relay open, thus maintaining system security.

Figure 3.6: Single Channel Relay Module

3.7 Key Pad

The Matrix Key Pad 4 x 4 is a compact input device featuring a 4x4 layout with 16 keys. Designed for reliability, it operates within a voltage range of 3V to 5V DC, making it suitable for various electronic projects. The keypad interfaces with microcontrollers via 8 digital pins (4 for rows and 4 for columns) and includes a female 2.54mm pitch connector for easy connectivity. Ideal for applications such as the Password-Based Circuit Breaker, this keypad provides a user-friendly solution for efficient control and interaction.

Figure 3.7: Key Pad

Specifications:

- **Key Layout**: 4 rows x 4 columns (16 keys total)
- **Key Type**: Membrane
- **Operating Voltage**: 3V - 5V DC
- **Interface**: 8 digital pins (4 for rows, 4 for columns)

6.8 Battery

The 3.7V Li-ion battery is a compact, rechargeable power source commonly used in portable electronics and embedded systems due to its high energy density and lightweight structure. In the this project, this battery provides reliable backup power to ensure the system remains operational during a power outage, maintaining functionality of key components such as the microcontroller,

LCD display, and keypad.

With a nominal voltage of 3.7V, Li-ion batteries are well-suited for low-power applications, delivering stable voltage levels for extended periods. They are rechargeable, typically lasting through hundreds of charge cycles, making them both economical and sustainable for projects requiring continuous or standby power. Additionally, their small size and lightweight construction allow easy integration into the project's housing without adding significant bulk.

Figure 3.8: li-ion battery

3.9 Buzzer

A buzzer is a simple electronic device that generates sound or an audible signal when an electrical current passes through it. Commonly used in alert systems, notifications, and alarms, buzzers are integral to various electronic devices due to their ability to provide immediate auditory feedback.

Figure 3.9: Buzzer

Buzzers consist of a coil of wire and a diaphragm. When current flows through the coil, it creates a magnetic field that moves the diaphragm, producing sound. The resulting sound is typically a "buzzing" or "clicking" tone. Most buzzers have two leads, often red (positive) and black (negative), and proper polarity is crucial for correct operation; reversing the connections can lead to no sound or distortion. In the context of this project, the buzzer serves as an alert mechanism for incorrect password entries, enhancing system security and user awareness.

3.10 220v to 5-volt adaptor

A 220 to 5-volt adapter, often referred to as a power supply or charger, is a device that converts electrical voltage from 220 volts to a lower voltage of 5 volts. This type of adapter is commonly used to power or charge electronic devices that require a 5-volt power source, such as smartphones, tablets, USB-powered devices, and various small electronics. The adapter takes the higher input voltage of 220 volts (which is a standard voltage level in many parts of the world, including Europe and Asia) and steps it down to a safer and compatible 5 volts for the connected

device. This is typically achieved through a transformer or other voltage conversion technology within the adapter.

Figure 3.10: 220v to 5-volt adaptor 220v to 5-volt adaptor

3.10 AC/DC Source

An AC/DC source refers to a power supply that provides electrical energy in either alternating current (AC) or direct current (DC) forms. These power sources are essential in various applications, including powering electronic circuits, appliances, and systems like the Password-Based Circuit Breaker.

- ✓ AC Source: The AC source delivers alternating current, which periodically reverses direction. This type of current is commonly used in household outlets and industrial settings because of its efficiency in long-distance transmission. In the context of the circuit breaker project, the AC source is used to power the electrical load that the circuit breaker controls.
- ✓ DC Source: In contrast, a DC source provides direct current, which flows consistently in one direction. This type of power supply is often used for low-voltage applications and is essential for powering microcontrollers and other components that require stable voltage, such as the Arduino Uno and LCD display in the Password-Based Circuit Breaker.

3.11 Jumper wire

It is possible to connect two places without soldering using jumper wires, which are wires with connector pins on either end. With breadboards and other prototype equipment, jumper wires make it easy to change circuits as needed. Despite the variety of colors available for jumper wires, the hues don't hold much meaning. Three types of jumper wire are commonly available: male-to-male, male-to-female, and female-to-female. Every wire has an endpoint that distinguishes it from the others. Male ends have a pin sticking out, which can be used to plug

into other items while female ends have a pin sticking out to be plugged into items.

Figure 3.11: Jumper wire

3.12 Design Specification

- Microcontroller: Arduino Nano, operating at 16 MHz, with 14 digital I/O pins (6 of which support PWM output) and 8 analog input pins. The Nano manages all input, output, and control operations in the system.
- Display: 16x2 Liquid Crystal Display (LCD), connected to the Arduino to show system status, password prompts, and feedback on operations.
- Power Supply: Combination of AC and DC sources, with an AC source powering the load and a DC source supplying stable power to the Arduino and connected components. A backup 3.7V Li-ion battery ensures uninterrupted operation during power outages.
- Relay Module: Single Channel Relay Module, designed to switch AC loads with low-power signals from the Arduino, enabling controlled on/off functionality.
- Input Interface: 4x4 Matrix Keypad, used for password entry to control access to the system.
- Booster Circuit: DC-DC booster circuit used to stabilize voltage levels, ensuring consistent performance across all system components.

- Software: Programmed using the Arduino IDE with C/C++ support, handling password verification, relay control, and display update.
- Housing: Enclosure with basic protection against dust and accidental contact, suitable for indoor use in controlled environments.
- Alert Mechanism: Piezo Buzzer, activated upon incorrect password entries to notify of unauthorized access attempts.

3.13 Summarization

This chapter has provided a detailed overview of the design and development process for the this project system, focusing on both hardware and software configurations. The system is designed to improve electrical safety by implementing a secure password-based access mechanism controlled by an Arduino Nano microcontroller. Key components such as a 4x4 keypad for password input, a 16x2 LCD for system feedback, and a single-channel relay for controlling the AC load work together to provide a reliable and user-friendly solution. A piezo buzzer alerts users to incorrect password attempts, enhancing security.

The system also integrates stable power management through AC and DC inputs, supported by a booster circuit and a backup battery to ensure continuous operation during power fluctuations. With the Arduino IDE managing the system's logic, including password verification, relay control, and alert generation, the "Password-Based Circuit Breaker" system offers a secure, efficient, and adaptable solution suitable for both residential and industrial applications.

CHAPTER FOUR

RESULTS AND DISCUSSIONS

4.1 Introduction

In this chapter, we present the outcomes and analysis of this project, examining the functionality, performance, and security aspects of the system. This section begins with an overview of the expected results, detailing the effectiveness of password-based control in managing AC loads and preventing unauthorized access. Through practical testing and simulations, we evaluate the system's responsiveness to password inputs, its stability under varied power conditions, and the performance of key components such as the relay, LCD, and buzzer. The discussion focuses on interpreting the observed results in relation to the initial design objectives, highlighting successes, potential improvements, and the overall impact on safety and user accessibility within electrical systems. ach test scenario is analyzed to assess the system’s efficiency in real-world applications, drawing conclusions on how well it meets the intended goals of secure, password-protected electrical load management. This chapter ultimately provides insights into the strengths and limitations of the design, along with recommendations for further enhancement.[12]

4.2 Result

we present *(Figure 4.1)* shows the setup of the "Password-Based Circuit Breaker" system, illustrating the key components such as the Arduino Nano microcontroller, the 4x4 keypad for password input,

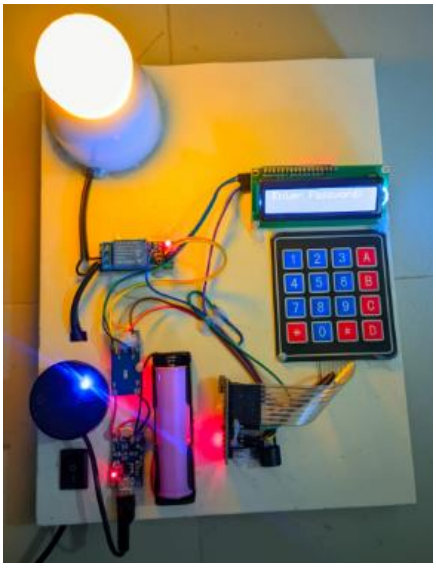

Figure 4.1: Project Picture

the 16x2 LCD display for system feedback, the relay module for controlling the AC load, and the buzzer for alerting incorrect password entries. During testing, the system demonstrated reliable functionality in controlling the AC load based on correct password inputs. When the correct password was entered, the relay successfully activated the AC load, allowing power flow. If the wrong password was input, the system responded by triggering the buzzer, effectively notifying the user of unauthorized access attempts.

The LCD displayed real-time information, including prompts for password entry and feedback messages for successful or incorrect attempts. The system maintained stable operation, even during simulated power fluctuations, thanks to the booster circuit and backup battery, ensuring the reliability and consistency of the password-based access control. These results confirm that the "Password-Based Circuit Breaker" system meets the design objectives, providing secure and efficient electrical load management while ensuring user-friendly interaction and operational reliability.

4.3 Outcome Analysis

The results of the **"Password-Based Circuit Breaker"** project were thoroughly tested and analyzed through various scenarios to evaluate the system's functionality and performance.

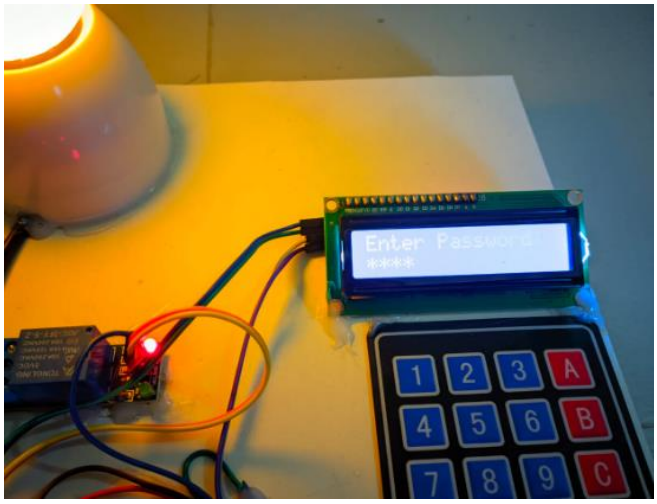

Figure 4.2: Enter Password

This figure *(fig-4.2)* demonstrates the user interface during the password input phase. The 4x4 keypad is used by the user to enter the password. As shown in the figure, the LCD screen displays a prompt for the user to enter the correct password. This visual feedback allows the user to interact with the system intuitively. The system waits for the correct password input to proceed with either activating or deactivating the circuit breaker.

In this image *(fig-4.3)*, the system has successfully received an incorrect password input. As a result, the system has triggered the buzzer alert, and the LCD displays an error message indicating that the password entered was incorrect. Additionally, the relay is in the "off" state, and the AC load is disconnected, ensuring that unauthorized users are unable to control the system. This failure response enhances the security of the system, preventing unauthorized access.

Figure 4.3: Breaker Off

In this figure *(fig-4.4)*, the correct password has been entered. The LCD shows confirmation of the correct password, and the relay is activated, turning the circuit breaker "on" and allowing power to flow to the AC load. This outcome verifies that the system is functioning as intended, with successful password verification enabling the relay control mechanism.

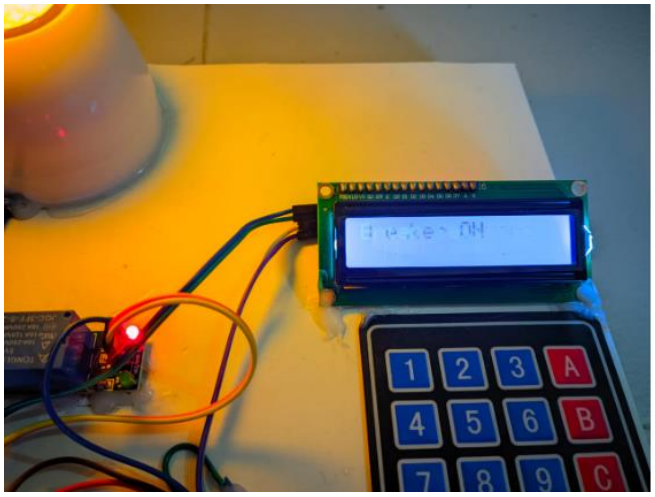

Figure 4.3: Breaker On

These outcomes confirm that the system performs as expected under different scenarios. It provides secure, password-protected control of electrical loads, ensuring that only authorized users can activate or deactivate the system. The integration of real-time feedback through the

LCD and the alert mechanism via the buzzer further improves the user experience and system security.

4.4 Advantages

- **Energy Efficiency:** The system enables selective control of electrical loads, ensuring that they are only active when authorized. This feature helps reduce unnecessary power consumption, potentially leading to cost savings on electricity bills.
- **Backup and Stability**: With the addition of a booster circuit and battery backup, the system remains stable during power fluctuations and continues to operate even during outages. This ensures consistent and reliable performance, particularly in environments where power control is critical.
- **Enhanced Security**: Requiring a password to activate or deactivate electrical loads minimizes the risk of unauthorized access. This added security protects against both accidental and intentional misuse, making the system especially valuable in sensitive environments like residential complexes, offices, and industrial facilities.
- **User-Friendly Interface:** The intuitive LCD display and keypad simplify interaction with the system, allowing users to easily input passwords and receive real-time feedback on the system's status. This ensures accessibility for users with varying technical expertise.
- **Reduced Risk of Electrical Hazards:** The circuit breaker mechanism cuts power to the load during unauthorized access attempts or system malfunctions. This safety feature helps prevent electrical accidents, safeguarding both users and equipment.
- **Adaptability and Flexibility**: The system's design allows it to be implemented across diverse applications, from household appliances to large-scale industrial machinery. With its microcontroller-based control, the system can be customized to suit specific user needs, making it versatile for various electrical load management scenarios.
- **Scalability**: The Password-Based Circuit Breaker can be easily expanded to incorporate additional features or support multiple loads, making it scalable for larger applications or future upgrades. The Arduino-based design provides flexibility for programming new functionalities as needed.
- **Ease of Maintenance**: With modular components like the relay, buzzer, and LCD display, the system is easy to troubleshoot and maintain. Individual components can be tested and replaced as necessary, ensuring minimal downtime and continued functionality.

- **Cost-Effective**: The Password-Based Circuit Breaker uses affordable, easily available components, making it a budget-friendly solution for both residential and industrial applications. Its simple design reduces long-term operational costs.

4.5 Disadvantages

- **Dependency on Password Security:** The system relies heavily on password protection for security. If the password is compromised or shared, unauthorized users may gain access, potentially undermining the safety benefits of the system.
- **Limited Protection Against Power Surges**: Although the system can control loads, it may not provide sufficient protection against high-voltage surges, which could damage components or connected devices. Additional surge protection may be required for full electrical safety.
- **Complexity in Setup and Configuration:** For those unfamiliar with microcontroller-based systems, setting up the components, wiring, and coding can be complex and time-consuming. This may require a learning curve for first-time users.
- **Sensitivity to Environmental Conditions:** Components like the LCD display, buzzer, and Arduino may be sensitive to environmental factors like moisture, dust, or extreme temperatures, which could impact their performance and durability over time.
- **Risk of Forgotten Password**: If users forget the password, access to the system could be disrupted, potentially leading to operational delays or the need for a reset procedure.

4.6 Discussion

In this project, successfully integrates key components such as the Arduino Nano, LCD display, relay module, and keypad to create a secure and efficient electrical load management system. The selection of reliable components ensures that the system is both functional and user-friendly, with the Arduino Nano acting as the core control unit for processing inputs and outputs. The relay module is crucial for securely switching the AC load, while the LCD display and keypad facilitate smooth user interaction for password entry and system feedback. The system's architecture is designed for optimal performance, with each component serving a specific role to maintain security and reliability. The circuit design ensures effective integration, with power management prioritized to prevent interference, and the programming logic provides secure password authentication, limiting access based on correct input. The inclusion of a booster circuit and backup battery further ensures consistent operation during power fluctuations. This

project not only enhances electrical safety by preventing unauthorized access but also demonstrates an effective integration of hardware and software to improve the management and control of electrical systems in residential, commercial, and industrial settings.

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATION

5.1 Conclusion

In conclusion, The **Password-Based Circuit Breaker** project successfully demonstrates an innovative approach to electrical load management by integrating password-protected access control into a circuit breaker system. Utilizing an Arduino Nano microcontroller as the central control unit, the system enhances security, operational safety, and user control. By requiring a password to activate or deactivate the AC load, the system reduces unauthorized access, which can help prevent accidental or intentional misuse of electrical systems. Key components, including a 4x4 keypad for password input, an LCD display for feedback, a relay for load control, and a buzzer for incorrect password alerts, work together to deliver a responsive, reliable, and user-friendly interface.

Through extensive testing, the project has validated the system's performance under various conditions, including power fluctuations, load changes, and different password scenarios. The integration of a booster circuit and backup battery has contributed to stable and uninterrupted operation, making the system adaptable to residential, commercial, and industrial environments. The project effectively addresses the risks associated with unauthorized access and aims to improve the safety and efficiency of electrical systems, particularly in applications where security and control are paramount. So, this serves as a significant step toward safer electrical management by providing a secure, adaptable, and user-centric solution. This project highlights the potential of combining digital control with conventional electrical components to enhance security and reliability, ultimately contributing to safer and more efficient electrical infrastructure

5.2 Limitations of the Work

The "Password-Based Circuit Breaker" project, like other security-focused systems, has several limitations that should be acknowledged:

- **Dependence on Accurate Password Entry**: The system relies on precise password input from the user. In cases where users enter incorrect passwords multiple times, the buzzer alert may become disruptive, and repeated entry could potentially lead to wear on the keypad. Adding an option for a secure reset or lockout feature could improve user experience and protect against accidental lockouts.

- **Environmental Sensitivity**: Key components such as the LCD display, keypad, and Arduino Nano may be vulnerable to environmental factors like moisture, dust, and temperature fluctuations. Such conditions could impact the durability and reliability of the system, potentially leading to component failure or reduced responsiveness over time, especially in outdoor or harsh industrial environments.
- **Limited Power Protection**: While the system includes a booster circuit and backup battery for power stability, it lacks a full surge protection mechanism. In the event of a high-voltage power surge, critical components like the relay or Arduino could be damaged, disrupting system functionality. Additional surge protection could improve the system's resilience but would increase cost and design complexity.
- **Scalability Constraints**: The current design, centered around the Arduino Nano, is effective for single-load applications but may face processing or memory limitations if expanded to handle multiple loads or complex functionalities. This limits its direct scalability for larger applications or environments requiring centralized control over several circuits.
- **Complexity for Non-Technical Users**: Setting up the components, wiring, and programming the system may pose challenges for individuals without a technical background. Any required maintenance or troubleshooting would likely require technical knowledge, potentially making the system less accessible to everyday users.
- **Maintenance Challenges**: In case of component failure, the modular setup of the system allows for individual replacements; however, diagnosing issues with the microcontroller or other electronic components may require specialized knowledge. The system's maintenance may therefore present challenges for non-technical users, requiring either professional assistance or additional training.
- **Cost Constraints for Advanced Features**: Additional features, such as surge protection, remote monitoring, or multi-user access, would increase the cost and complexity of the system. While these improvements could enhance functionality, the added expense might limit its accessibility for budget-conscious applications, particularly in residential or small-scale environments.
- **Limited Scalability**: The system is designed for single load control, and expanding it to manage multiple loads or larger systems may require additional modifications and complexity, impacting cost and design.

5.3 Future Recommendation

To enhance the functionality and applicability of the "Password-Based Circuit Breaker" system, one key improvement would be the integration of remote monitoring and control. By incorporating wireless technologies such as Wi-Fi or Bluetooth, users would have the ability to remotely access and control the circuit breaker from smartphones or computers. This would make the system more convenient, especially in large-scale or hard-to-reach installations, such as industrial environments or residential complexes where physical access is limited. Another area for improvement is supporting multiple loads. Currently, the system is designed to control a single electrical load. However, expanding the system to manage multiple loads simultaneously would make it more applicable for larger applications, such as offices or industrial settings. This can be achieved by integrating multi-channel relays and enhancing the power management capabilities of the system, allowing users to control several devices or appliances from one central unit. Advanced security measures are another important recommendation for future development. While the current password-based security mechanism is effective, integrating two-factor authentication (2FA**)** or biometric verification, such as fingerprint recognition, would provide an extra layer of protection. This would be especially important in environments where the electrical system needs to be highly secure to prevent unauthorized access or tampering.

Furthermore, the integration of smart grid compatibility is a potential upgrade that would optimize energy use. By enabling the system to communicate with a smart grid, the circuit breaker could automatically adjust based on real-time power demand and grid conditions. This would contribute to more efficient energy management and reduce operational costs, especially in large-scale applications where energy consumption is a key concern. Lastly, improvements to user interface and power protection can also be considered. Upgrading the system with a touchscreen interface or voice control could make it more accessible, while adding surge protection and voltage regulation would protect the system and connected devices from power spikes, ensuring its reliability and longevity.

REFERENCES

[1] Mathavan, N., Praveena, B., Reenasri, V. And Sakthilakshmi, M., 2019. Electrical Line Man Safety Using Android Based Circuit Breaker. Int J Recent Trends Eng Res (IJRTER), ISSN (Online), Pp.2455-1457. Doi:10.1007/S12652-020-02618-1.

[2] Ganesh Krishna Naik,Srikanth N,Vinod Kumar KM,Rajeshkar Vs "PASSWORD BASED CIRCUIT BREAKER",IJAEEE,Dr.Ambedkar Institute Of Technology.IJAEEE,Vol-5,Pp. 17 To 19,Issue 6-2016.

[3] Olalekan Oyebola , "PASS WORD BASED ELECTTRIC LOAD SWITCHING GEAR FOR THE SAFETY OF LINEMAN",Department Of Computer Engineering Technology,Gate Way (ICT) Polytechnic Saapade,Nigeria.IJOEST ,Vol 1,Pp. 48 To 55 ,Issued 05-2017.

[4] Athira P.Nair ,Josephin,A.Anjana,C.Athira,Sebin Jolika, "ELECTRIC LINE MAN SAFETY SYSTEM WITH OTP PASSWORD BASED CIRCUIT BREAKER",BTC College Of Engineering ,Koothattukulam.IJRET,Vol-4,Pp.2319 To 1163, Issued Aprl-2015.

[5] Olalekan Oyebola , "PASS WORD BASED ELECTTRIC LOAD SWITCHING GEAR FOR THE SAFETY OF LINEMAN",Department Of Computer Engineering Technology,Gate Way (ICT) Polytechnic Saapade,Nigeria.IJOEST ,Vol 1,Pp. 48 To 55 ,Issued 05-2017.

[6] Kumar, Jay, et al. "Password based circuit breaker." International Journal of Recent Research Aspects 3.1 (2016): 80-85.

[7] Gautam, Yash Pal. "Password based circuit breaker with GSM module." International Journal of advanced research, Ideas and Innovations in Technology 3.3 (2017): 1460-1464.

[8] Mahalle, Radhika Motiram, Adhirath Kohale, Pratik Raikar, Bhagavati Goswami, and Shreyash Dhawale. "password base circuit breaker using GSM modem." IRE Journals 4, no. 12 (2021).

[9] Onwuemeodo, C.L., Duru, C., Anyasodor, C.C. and Obiefule, N.D., 2022. Design and construction of Internet of Things (IoT) password based circuit breaker. Journal of Electrical Engineering, Electronics, Control and Computer Science, 8(3), pp.43-48.

[10] Hudedmani, Mallikarjun G., Nitin Ummannanavar, Mani Dheeraj Mudaliar, Chandana Sooji, and Mala Bogar. "Password based distribution panel and circuit breaker operation for the safety of lineman during maintenance work." Advanced Journal of Graduate Research 1, no. 1 (2017): 35-39.

[11] Sharma, Ritik, Pulusu Srinivas Reddy, and Vineet Kumar. "PASSWORD BASED CIRCUIT BREAKER." (2021).

[12] Manivannan, S., Sudhahar, S., Oorappan, G.M., Rajalashmi, K. and Saravanakumar, N., 2021. Design Implementation and Evaluation of Password Protected Circuit Breaker for Reliable Power System Protection and Maintenance. In Advances in Materials Research: Select Proceedings of ICAMR 2019 (pp. 933-942). Springer Singapore.

[13] Kanagalakshmi, K., R. Aarthi, S. Devi Priya, and S. Gnanasambanthan. "Design and implementation of password and fingerprint-enabled circuit breaker using Arduino, IoT and GSM." In Computational Methods in Science and Technology, pp. 270-276. CRC Press, 2024.

[14] Sivakumar, Krishna Veni Kaliappan, Arun Balaji Anandha Krishnan, Arun Saravanan Valliappan, and Karputha Pandi Periyaandar. "Electric line man safety with fingerprint and password based circuit breaker." In AIP Conference Proceedings, vol. 2831, no. 1. AIP Publishing, 2023.

[15] Rahim, M.N.A. and Bohari, A.A., 2022. Password Code and Fingerprint Based Security Using Relay. Progress in Engineering Application and Technology, 3(2), pp.520-532.

[16] Raza, Wasiq, and Naitam MD. "A.:"Electric lineman protection using user changeable password based circuit breaker"." Int. J. Res. Sci. Eng 3.2 (2017).

APPENDIX

```
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
#include <Keypad.h>
// LCD settings
LiquidCrystal_I2C lcd(0x27, 16, 2);  // Change 0x27 to your LCD's address if necessary
// Keypad settings
const byte ROWS = 4;
const byte COLS = 4;
char keys[ROWS][COLS] = {
  {'1', '2', '3', 'A'},
  {'4', '5', '6', 'B'},
  {'7', '8', '9', 'C'},
  {'*', '0', '#', 'D'}
};
byte rowPins[ROWS] = {5, 6, 7, 8}; // Connect to the row pinouts of the keypad
byte colPins[COLS] = {9, 10, 11, 12}; // Connect to the column pinouts of the keypad
Keypad keypad = Keypad(makeKeymap(keys), rowPins, colPins, ROWS, COLS);
// Password settings
const String password = "1234"; // Change this to your desired password
String inputPassword = "";
bool ledState = false;
const int Relaypin = 4; // Pin connected to the LED
const int buzzerPin = 13; // Pin connected to the buzzer
```

```
void setup() {
 lcd.init();
  lcd.backlight();
  pinMode(Relaypin, OUTPUT);
  pinMode(buzzerPin, OUTPUT);
  digitalWrite(Relaypin, LOW);
  lcd.setCursor(0, 0);
  lcd.print("Enter Password:");
}
void loop() {
  char key = keypad.getKey();

  if (key) {
    // Beep the buzzer when any key is pressed
    tone(buzzerPin, 1000, 100); // 1000 Hz for 100 ms
    if (key == 'D') {
      // Check if the input password is correct
      if (inputPassword == password) {
        ledState = !ledState; // Toggle LED state
        digitalWrite(Relaypin, ledState ? HIGH : LOW);
        lcd.clear();
        lcd.print(ledState ? "Breaker ON" : "Breaker OFF");
      } else {
        lcd.clear();
        lcd.print("Wrong Password");
      }
      delay(2000);
```

```
      lcd.clear();
      lcd.print("Enter Password:");
      inputPassword = ""; // Reset input
    } else if (key == 'C') {
      inputPassword = ""; // Clear input
      lcd.clear();
      lcd.print("Enter Password:");
    } else {
      inputPassword += key; // Append key to input password
       // Display asterisks for each entered character
      lcd.clear();
      lcd.print("Enter Password:");
      lcd.setCursor(0, 1); // Move cursor to the second line

      for (int i = 0; i < inputPassword.length(); i++) {
        lcd.print('*'); // Print asterisk for each character in inputPassword
      }
    }
  }
}
```