Design and Implementation of an IoT-Based Circuit Breaker with Password Security for Enhanced Electrical Safety and Control

Shamshad Ansari [1], Shifa Bano [2], Ankesh Kumar Yadav [3]
[1,2,3] *Buddha Institute of Technology,Gida, Gorakhpur*

***Abstract*—This research presents the design and implementation of an IoT-based circuit breaker system integrated with password security to enhance electrical safety and control. The system leverages IoT technology for remote monitoring and predictive maintenance while minimizing human interaction with high-voltage circuits. Password authentication ensures secure access, preventing unauthorized usage. Experimental testing demonstrated high reliability, fast relay response, and cost-effectiveness, making the system scalable for residential and industrial applications.**

***Index Terms*—IoT, Circuit Breaker, Password Security, Electrical Safety, Remote Monitoring, Predictive Maintenance, Arduino Uno, ESP8266, Relay Module, Real-Time Data.**

I. INTRODUCTION

Electrical safety remains a critical concern, especially for maintenance workers exposed to high-voltage systems. Traditional circuit breakers lack remote operability and secure access control, leading to risks such as miscommunication and unauthorized tampering. To address these challenges, this research presents an IoT-based circuit breaker integrated with password security. The system enables remote operation, enhances safety, and provides real-time monitoring through IoT technology, while password protection ensures secure access and prevents unauthorized use

1.1 Relevance:

This project addresses critical safety concerns in electrical systems by minimizing direct human interaction with high-voltage circuits through remote operability. The integration of IoT and password security prevents unauthorized access while enabling real-time monitoring and predictive maintenance. Its scalable design makes it a significant contribution to both residential and industrial electrical safety.

1.2 Problem Statement:

Traditional circuit breakers pose risks to maintenance workers due to the lack of remote operability and secure access control. Miscommunication or unauthorized tampering increases the likelihood of accidents. This project aims to address these challenges by developing a cost-effective IoT-enabled circuit breaker with password security, enhancing safety, accessibility, and system management.

1.3 ObjectivesEnhance:

- Enhance Electrical Safety: Minimize direct human interaction with high-voltage circuits through remote operability.
- Secure Access Control: Prevent unauthorized usage via password-protected mechanisms.
- Enable Real-Time Monitoring: Utilize IoT for continuous data collection and fault detection.
- Implement Predictive Maintenance: Leverage sensor data to anticipate and prevent system failures.
- Scalable Design: Ensure adaptability for both residential and industrial applications.

1.4 Scope:

This project focuses on designing an IoT-based circuit breaker system with password security, aiming to improve electrical safety and remote accessibility. The system is scalable for both residential and industrial applications, integrating hardware like microcontrollers, sensors, and relays with IoT connectivity for real-time monitoring and predictive maintenance. It addresses the need for secure and efficient electrical control while minimizing human interaction with high-voltage circuits.

2. LITERATURE REVIEW

The integration of IoT into electrical systems has significantly enhanced safety and operational efficiency. Studies, such as Lee & Park (2024), emphasize the role of secure IoT-based circuit breakers in reducing accidents and improving access control. Advancements in microcontroller technology (e.g., Arduino), IoT communication modules (e.g., ESP8266), and password authentication systems have laid the groundwork for innovative solutions in electrical safety. This project builds upon these studies by combining IoT connectivity and a keypad-based security layer to address existing challenges effectively.

3. SYSTEM DESIGN AND METHODOLOGY

The system integrates hardware and software components to create a secure IoT-based circuit breaker. Key hardware includes an Arduino Uno microcontroller, sensors for current, voltage, and temperature monitoring, a 4x4 keypad for password authentication, a 4-channel relay module for electrical switching, and an ESP8266 Wi-Fi module for IoT connectivity. The software, developed in Arduino IDE using C/C++, incorporates libraries for sensor handling, password validation, and MQTT communication for secure data transmission. A web interface built with HTML and JavaScript enables remote monitoring and operation.

The methodology followed a structured approach:

1. Requirement Analysis: Identified needs for enhanced electrical safety and secure access control.
2. Hardware Prototyping: Assembled and tested key components to ensure seamless integration.
3. Software Development: Programmed the microcontroller and developed the web interface.
4. Testing: Conducted unit testing, integration testing, and security validation.
5. Deployment: Finalized the system design for residential and industrial scalability.

3.1 Design Overview:

The system integrates hardware and software components to create a secure and efficient IoT-based circuit breaker. Key hardware includes an Arduino Uno microcontroller, a 4-channel relay module, a 4x4 keypad for password authentication, sensors for monitoring electrical parameters, and an ESP8266 Wi-Fi module for IoT connectivity. The software is developed using C/C++ in Arduino IDE and incorporates MQTT protocols for secure data communication. A user-friendly web interface facilitates remote operation and monitoring, ensuring accessibility and enhanced electrical safety.

3.2 ComponentsArduino Uno:

The Arduino Uno serves as the central processing unit in the IoT-based circuit breaker system. It handles data acquisition from sensors, processes password inputs from the keypad, and controls the relay module for switching electrical circuits. Its compatibility with the ESP8266 Wi-Fi module ensures seamless IoT connectivity for remote monitoring and operation. The simplicity and reliability of the Arduino Uno make it ideal for prototyping and real-world applications.

3.3 Circuit Design:

The circuit integrates an Arduino Uno microcontroller with sensors (current, voltage, temperature), a 4-channel relay module for electrical switching, and a 4x4 keypad for password input. The ESP8266 module facilitates Wi-Fi connectivity for IoT-based remote monitoring and control. All components are interconnected on a breadboard, ensuring seamless communication between hardware elements.

3.4 Software Development:

The microcontroller was programmed using the Arduino IDE, leveraging C/C++ for firmware development. Libraries for handling sensor data, password authentication, and relay control were integrated. MQTT protocols ensured secure data transmission between the IoT system and remote interface. A web interface, designed with HTML and JavaScript, provided an intuitive platform for remote monitoring and control.

3.5 Methodology:

The development of the IoT-based circuit breaker system followed a structured approach:

1. Requirement Analysis: Identified the need for enhanced electrical safety and secure access control.
2. Hardware Prototyping: Assembled components like Arduino Uno, 4-channel relay, 4x4 keypad,

ESP8266, and sensors to ensure seamless integration.

3. Software Development: Programmed the microcontroller using C/C++ in Arduino IDE, incorporating libraries for sensor data handling, password authentication, and MQTT-based IoT communication.
4. Testing: Conducted unit testing for individual components, integration testing for overall functionality, and security testing to validate password protection mechanisms.
5. Deployment: Finalized the system design for residential and industrial scalability.

4. IMPLEMENTATION

The IoT-based circuit breaker system was implemented using an Arduino Uno microcontroller interfaced with sensors (current, voltage, temperature), a 4-channel relay module, a 4x4 keypad for password input, and an ESP8266 Wi-Fi module for IoT connectivity. The hardware was assembled on a breadboard, ensuring seamless integration and testing. Software development, utilizing the Arduino IDE and MQTT protocols, enabled secure data transmission and effective remote monitoring. A user-friendly web interface, built with HTML and JavaScript, allowed for intuitive system control.

4.1 Hardware Setup:

The hardware consists of an Arduino Uno microcontroller interfacing with a 4-channel relay module, sensors (current, voltage, temperature), and a 4x4 keypad for password input. The ESP8266 Wi-Fi module enables IoT connectivity, and components are assembled on a breadboard for integration and testing. This configuration ensures seamless functionality and real-time monitoring.

4.2 Software Configuration:

The Arduino IDE was utilized to program the microcontroller, incorporating libraries for keypad input, sensor communication, and Wi-Fi connectivity. MQTT protocols were implemented to ensure secure and reliable data transmission between the IoT components and the remote interface. The web interface, developed using HTML and JavaScript, provided an intuitive platform for remote control and monitoring.

4.3 TestingUnit Testing:

Each component of the IoT-based circuit breaker system was rigorously tested to ensure individual functionality. The relay module reliably switched circuits with a success rate of 99.8% across 1000 operations. Sensors accurately monitored electrical parameters, including current, voltage, and temperature. Password validation was successfully implemented, preventing unauthorized access during repeated attempts. These results confirm the robustness and reliability of all system components.

5. RESULTS AND DISCUSSION

The IoT-based circuit breaker system demonstrated high reliability and effectiveness during testing. Sensor readings were consistent, with current averaging 10.5A and spikes up to 12A triggering the relay within 50ms, achieving a 99.8% success rate over 1000 operations. Voltage remained stable at 230V, and temperature peaked at 27°C under load conditions.

The system’s integration of IoT enabled seamless remote monitoring and control, enhancing safety by minimizing direct human interaction with high-voltage circuits. Predictive maintenance capabilities further reduced downtime and operational costs. However, challenges such as cybersecurity risks and reliance on stable internet connectivity highlight areas for improvement. Future enhancements, including advanced encryption and offline functionality, could address these limitations.

5.1 Measurement DataSensor Readings:

During testing, the system monitored electrical parameters effectively:

- Current: Averaged 10.5A, with spikes up to 12A, triggering relay disconnection.
- Voltage: Remained stable at 230V throughout operation.
- Temperature: Peaked at 27°C under load conditions.

These results validate the system's reliability and responsiveness in real-time monitoring and fault detection.

5.2 Performance Analysis:

The IoT-based circuit breaker with password security demonstrated high reliability and efficiency during

testing. The system's relay response time was 50ms, achieving a 99.8% success rate across 1000 operations. Sensors effectively monitored current, voltage, and temperature, ensuring prompt detection of anomalies, such as current spikes of 12A triggering immediate circuit disconnection. The IoT-enabled web interface provided seamless remote control and monitoring, though stable Wi-Fi connectivity was essential. Overall, the system proved to be a robust and cost-effective solution for enhancing electrical safety and control.

5.3 Discussion:

The IoT-based circuit breaker with password security addresses critical issues of electrical safety and access control. By reducing the need for direct interaction with high-voltage systems, it significantly enhances operational safety. The incorporation of IoT enables real-time monitoring and predictive maintenance, contributing to system reliability and cost efficiency. However, potential challenges such as dependence on stable internet connectivity and cybersecurity risks require attention. Future iterations could include advanced encryption techniques and offline functionality to mitigate these issues. Overall, the system proves to be a practical and innovative solution for modern electrical management.

6. CONCLUSION

The IoT-based circuit breaker with password security successfully enhances electrical safety, access control, and operational efficiency. The integration of IoT technology enables remote monitoring and predictive maintenance, while password protection ensures secure access. The system proves to be a reliable and cost-effective solution for both residential and industrial applications, addressing key challenges in modern electrical management.

6.1 Summary:

This study presents the design and implementation of an IoT-based circuit breaker system featuring password security for enhanced electrical safety and control. The system leverages IoT connectivity for remote monitoring and operation, combined with a password-protected access mechanism to prevent unauthorized usage. Experimental results demonstrate high reliability, fast relay response, and improved safety through predictive maintenance, making it a scalable and cost-effective solution for residential and industrial applications.

6.2 Contributions:

The IoT-based circuit breaker system with password security enhances electrical safety by reducing the need for direct human interaction with high-voltage circuits. It introduces secure access control through password authentication and offers real-time monitoring and predictive maintenance via IoT integration. The system demonstrates high reliability and cost-effectiveness, making it a scalable solution for residential and industrial applications.

6.3 Future Work:

To build upon the achievements of this project, several enhancements and extensions can be considered for future work:

1. Multi-Factor Authentication Incorporating multi-factor authentication, such as fingerprint or facial recognition, alongside password security, could further bolster access control and enhance the overall security of the system.
2. Machine Learning Integration Leveraging machine learning algorithms for predictive maintenance can improve fault detection and system reliability. This approach could enable the identification of potential issues before they escalate into critical failures.
3. Industrial Scalability Expanding the system's scalability for industrial applications would make it suitable for high-power systems and large-scale operations. Integration with industrial protocols like Modbus or PROFIBUS could ensure seamless compatibility.
4. Advanced Encryption Techniques Implementing advanced encryption methods for IoT data transmission would mitigate cybersecurity risks, ensuring secure communication even under malicious attacks.
5. Offline Functionality Developing offline capabilities, such as local storage and operational backups, would allow the system to function independently of internet connectivity, ensuring reliability in remote or unstable network conditions.

Enhanced User Interface Refining the web and mobile interfaces to include real-time analytics dashboards

and customizable notifications would enhance usability and accessibility for end-users.

REFERENCES

[1] Lee, K., & Park, S. (2024). Secure IoT-Based Circuit Breaker Systems. Journal of Electrical Engineering, 45(3), 123–134.
[2] Smith, J., & Doe, A. (2023). Internet of Things: Security and Applications. Springer.
[3] Arduino. (2023). Arduino Uno Rev3 Technical Documentation.