PROGRESS IN ENGINEERING APPLICATION AND TECHNOLOGY
e-ISSN: 2773-5303

PEAT

Vol. 7 No. 1 (2026) 267-281
https://publisher.uthm.edu.my/periodicals/index.php/peat

# IoT-Enabled Automated Circuit Breaker with Password Protection for Smart Homes using Arduino and ESP8266

**Lee Kuan Pang[1], Mohd Fadly Abd Razak[1]***

[1] *Department of Electrical Engineering Technology, Faculty of Engineering Technology University Tun Hussein Onn Malaysia, Hab Pendidikan Tinggi Pagoh, KM 1, Jalan Panchor, Panchor, 84600, MALAYSIA*

*Corresponding Author: fadly@uthm.edu.my
DOI: https://doi.org/10.30880/peat.2026.07.01.031

**Article Info**

Received: 12 January 2026
Accepted: 20 February 2026
Available online: 25 May 2026

**Keywords**

IoT, ESP8266, Smart Home, Smart Circuit Breaker, Overcurrent Protection, Overvoltage Protection, Password-Based Access Control

**Abstract**

The Internet of Things (IoT) has enabled the development of smart home systems that improve safety, monitoring, and user control of residential electrical installations. The basic protection system operates through conventional circuit breakers which protect against electrical faults but it fails to provide real-time monitoring and remote access and secure operation. This study presents the development of an IoT-enabled automated circuit breaker with password protection for smart home applications. The proposed system aims to improve electrical safety through real-time monitoring, secure access control, and automatic fault protection. The system operates through an Arduino Mega 2560 microcontroller which connects to an ESP8266 Wi-Fi module and ACS712 current sensor and ZMPT101B voltage sensor and relays and keypad and LCD and Blynk mobile application. Electrical parameters such as current and voltage are continuously monitored to detect abnormal operating conditions. When predefined thresholds are exceeded, the system automatically trips the circuit and sends instant alerts to users via the Blynk platform. Experimental results demonstrate accurate current and voltage detection, fast fault response, and reliable remote monitoring and control, confirming the effectiveness of the proposed system as a smart circuit breaker solution for enhancing electrical safety in modern smart homes.

## 1. Introduction

Smart home environments have become increasingly common due to the widespread adoption of connected electrical devices and remote-control systems. The integration of electrical loads with Internet of Things (IoT) devices and wireless connectivity systems creates new electrical safety and system security challenges. Electrical faults such as overloads, short circuits, overvoltage conditions, and unauthorized circuit switching can lead to equipment damage, power interruptions, and potential residential fire hazards.

A circuit breaker functions as an essential electrical system component which protects devices from damage and fire risks by stopping excessive electrical currents. The traditional operation of circuit breakers requires manual activation while these devices provide basic protection without any additional capabilities. Smart circuit breakers have become popular because Internet of Things (IoT) technology allows users to control them from a distance while tracking their energy use and making operations more user-friendly. Home automation systems became completely transformed through IoT technology because users can now operate their electrical systems from any location while keeping their systems protected through smart circuit breakers which include built-in security measures [1]. The research employs an Arduino Mega 2560 which functions as the primary microcontroller to track and manage home electrical systems while the ESP8266 Wi-Fi module provides Internet of Things (IoT) access for distant control. Users can control various electrical devices through Blynk mobile app controls which establish wireless networks to deliver an easy smart home electrical system management solution that keeps security intact [2].

Existing residential electrical protection systems contain a major weakness because they lack real-time monitoring and remote access and authentication systems. The combination of unauthorized circuit operation with delayed fault detection and missing real-time system information leads to two main problems which include increased energy waste and safety risks. The present system shows multiple deficiencies which demand the development of a better circuit breaker solution that connects Internet of Things (IoT) capabilities with secure entry systems and automated fault detection mechanisms.

This project addresses these challenges by developing an IoT-enabled automated circuit breaker system with password protection. The proposed system enables remote monitoring and control of residential electrical circuits while preventing unauthorized operation. By incorporating real-time current and voltage monitoring with automated protection mechanisms, the system enhances electrical safety and provides rapid response to abnormal operating conditions in smart home applications.

## 2. Related Works

Researchers have performed multiple studies which investigate smart automated circuit breaker systems that operate through embedded platforms when combined with Internet of Things technology. The existing research base enables developers to establish protected electrical defense systems which smart homes need for remote operation.

Kumar et al. developed a smart application-based circuit breaker which uses a protected password system to boost safety measures for electrical workers who perform maintenance tasks. The system depends on an Arduino Uno, which wasATmega328 which works with keypad password verification and LCD screen and relay controls and GSM technology to enable distant system management [3]. The control of the circuit breaker depends on authorized personnel who enter a secret passcode which protects against unintentional power activation. The system creates better security and safety for linemen, but its operation depends on GSM communication which might cause network-related delays and connectivity challenges [3].

Kalaimani et al. developed an IoT-based circuit breaker controller which enables disabled people to operate their home appliances through remote control methods. The system operates through an Arduino microcontroller which connects Wi-Fi and relay modules and Blynk mobile application for remote control and monitoring [4]. The results demonstrated successful real-time switching of appliances using a smartphone interface. The research centers on accessibility but it fails to include electrical parameter monitoring which would detect faults through voltage and current sensing [4].

Srivathsan et al. created a smart circuit breaker which operates through GSM and Arduino technology and uses One-Time Password (OTP) authentication to improve its operational safety [5]. The system employs an Arduino Uno together with a GSM module and keypad and LCD and relay modules to enable breaker operation only through users who have permission. The security system which depends on OTP for control surpasses static password protection, yet it depends on GSM network availability and fails to deliver real-time electrical parameter monitoring through IoT dashboard interfaces [5].

Yadav and Sharma developed a Smart MCB system which integrates embedded systems with IoT technology to solve the restrictions found in traditional miniature circuit breakers [6]. The system uses a NodeMCU microcontroller together with voltage sensors and relays and an LCD display and IFTTT for IoT automation to send email alerts when voltage levels become too high. The system will automatically disconnect appliances whenever voltage levels rise above the established safety limits. The system provides voltage protection through its design, yet it lacks both password-based access control and complete current monitoring capabilities [6].

Progress in Engineering Application and Technology Vol. 7 No. 1 (2026) p. 267-281

Siregar and Tandry presented a smart home monitoring and control system using the Blynk application [7]. The system enables users to monitor their home electrical parameters through real-time data display while they can operate their appliances from any location through the NodeMCU ESP32 system which connects different sensors. The study confirms reliable real-time monitoring and notification features; however, it is designed as a general smart home system and does not specifically focus on circuit breaker protection or authentication mechanisms [7].

Sahabudin et al. developed a real-time electrical monitoring system for residential buildings using IoT technology [1]. The system combines ACS712 current sensors with ZMPT101B voltage sensors and ESP32 microcontroller and cloud platforms ThingSpeak and Blynk to display data. The results show accurate voltage and current monitoring with real-time alerts. The system provides powerful monitoring functions, yet it lacks automatic circuit shutdown and password-based management systems [1].

## 3. Methodology

The research followed a development-based experimental strategy to create and test an automated circuit breaker system which operates through IoT technology for smart home use. The research method required researchers to join hardware elements including a microcontroller and current and voltage sensors and relays and communication modules to software code and an IoT monitoring system. During the testing phase the system underwent assembly followed by programming and evaluation under normal and abnormal operating conditions to check its operational performance and safety measures and reliability. The overall approach ensured that the proposed system could achieve secure remote control, real-time monitoring, and automatic fault protection as intended.

### 3.1 Materials

The project built an IoT-enabled automated circuit breaker system through the strategic combination of multiple hardware components and software platforms. The project's hardware components included an Arduino ATMEGA 2560 microcontroller and an ESP8266 Wi-Fi module and ACS712 current sensors and ZMPT101B voltage sensors and relay modules alongside a keypad and an LCD display. Three software tools including Arduino Integrated Development Environment (IDE) for programming and Blynk application for remote monitoring and control and Fritzing software for circuit design supported the project. System assembly along with programming and testing operations needed a digital multimeter and soldering iron along with a breadboard and jumper wires and a personal computer.

### 3.2 System Block Diagram

The system block diagram presented in Figure 1 illustrated the operation of the IoT-enabled automated circuit breaker controlled by the Arduino ATMEGA 2560. The AC voltage sensor receives power from the AC power supply, and each load line receives protection from an MCB and measurement through separate AC current sensors. The system transmits the detected voltage and current readings to the Arduino for ongoing monitoring and fault detection purposes. The Arduino system uses measured parameters to operate the main AC relay and individual AC relays which control the power flow to Load 1, Load 2 and Load 3. The ESP8266 Wi-Fi module enables communication between the system and the Blynk mobile application for remote monitoring and control. A keypad serves as the password-protected user input interface and the system status information shows up on the LCD display. The setup provides secure instant monitoring and automated protection for multiple electrical loads in real time.

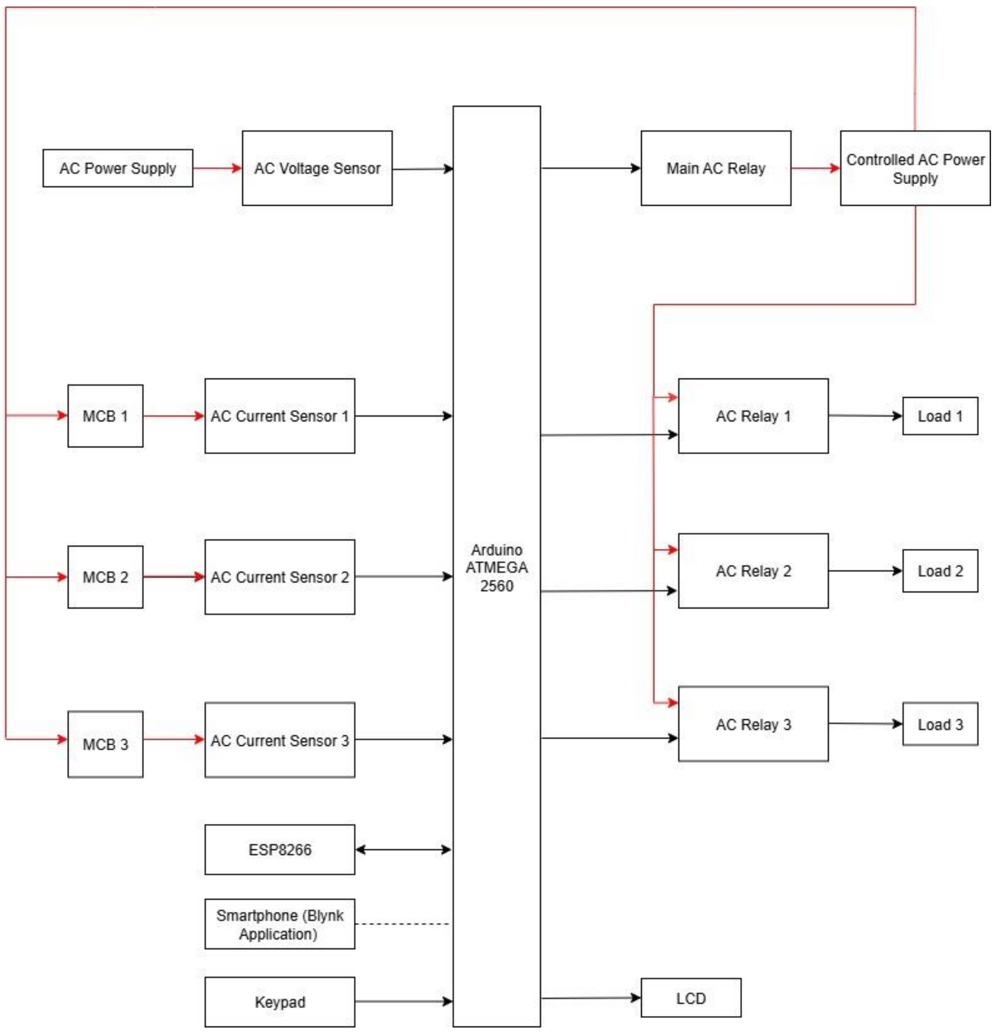
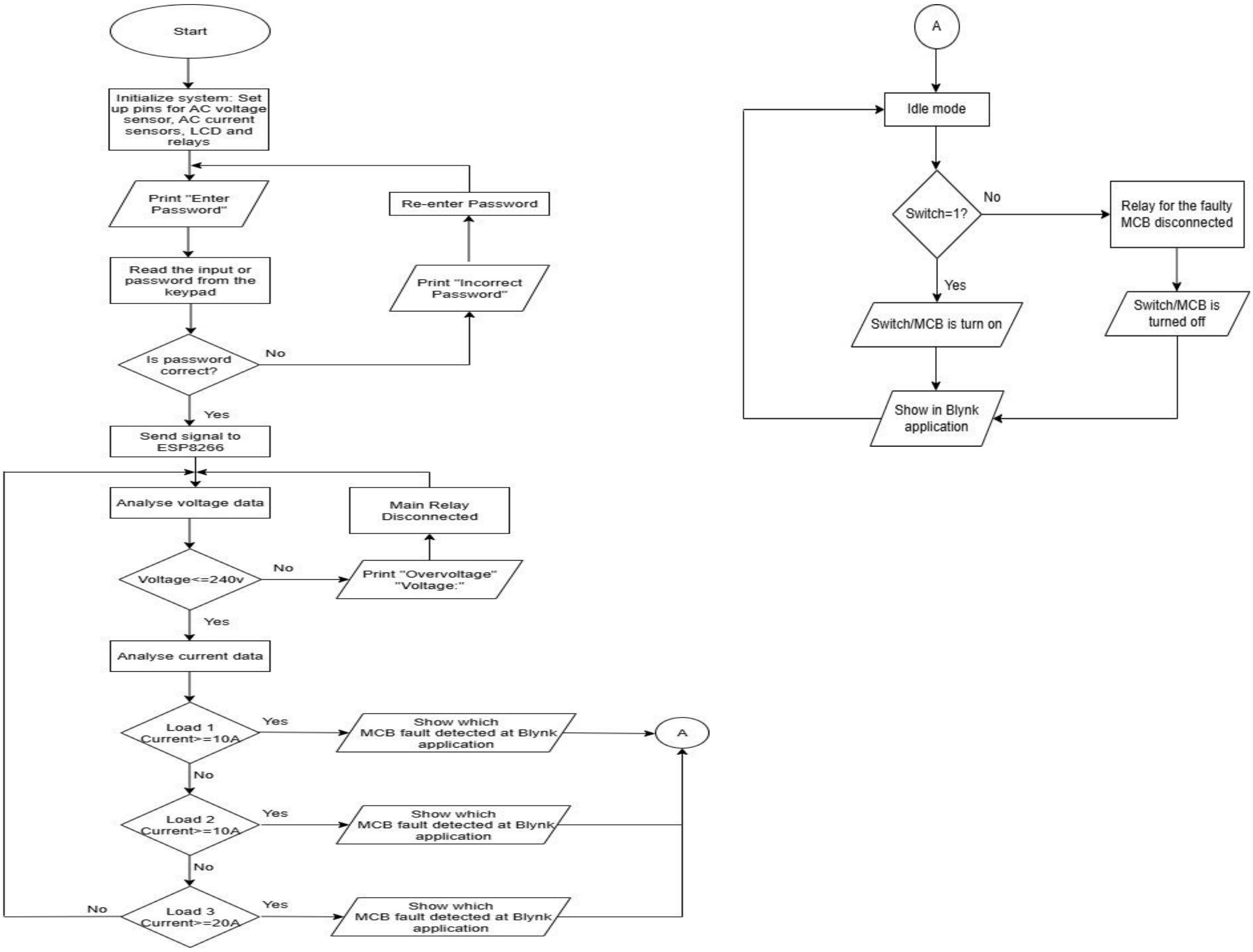



**Fig. 1** *System Block Diagram*

## 3.3 System Flowchart

The system flowchart presented in Figure 2 demonstrated the step-by-step operation of the IoT-enabled automated circuit breaker system. The system initialization process started with password verification through the keypad which provided secure access to the system. The system verified operating safety through AC voltage level analysis after authentication with the ESP8266 module. The main relay would disconnect itself if an overvoltage condition appeared to protect the system from damage. The system performed load current analysis at normal voltage levels to match the results against established threshold values. The Blynk application displayed the fault status after the system detected an overcurrent fault and identified the faulty MCB. The system operated in idle mode after startup so users could control it while the system monitored electrical conditions.




**(a)** **(b)**

**Fig. 2** *(a) System Flowchart; (b) Continue of System Flowchart*

## 3.4 Circuit Diagram

The circuit diagram presented in Figure 3 demonstrated all electrical connections which form the complete IoT-enabled automated circuit breaker system. The main controller for this system operates through Arduino ATMEGA 2560 which connects to ZMPT101B AC voltage sensor for supply voltage monitoring. Three ACS712 current sensors were connected in series with each load line after the respective MCBs to measure load currents. The voltage and current signals which were measured connected to the Arduino analogue input pins to enable ongoing signal monitoring. The ESP8266 Wi-Fi module was connected to the Arduino via serial communication to enable data transmission and remote monitoring through the Blynk application. The main SSR-40DA relay served as the control unit for the entire AC power system but individual SSR-40DA relays operated Load 1 and Load 2 and Load 3 under standard and emergency situations. A keypad was used to provide password-based user input, and an I2C LCD was used to display system status and warning messages. The circuit design provided protected control functions and real-time monitoring and automatic protection for several AC loads.

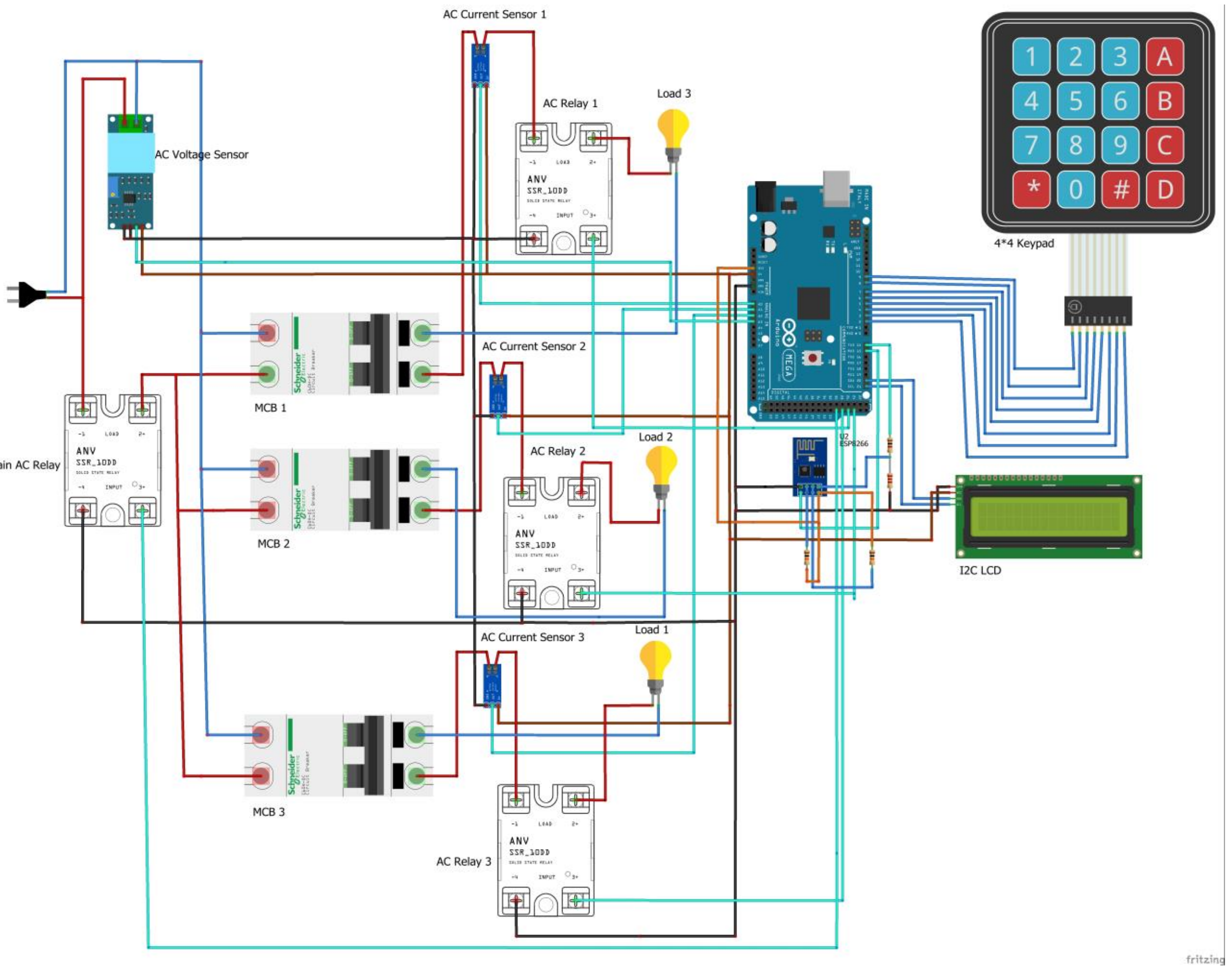



**Fig. 3** *Circuit Diagram*

## 3.5 Blynk Interface

The Blynk interface presented in Figure 4 functions as the IoT platform which provides users with the capability to monitor and operate the automated circuit breaker system from remote locations. The interface was set up to show live electrical data which includes AC voltage and load current and circuit status and fault alerts from the ESP8266 Wi-Fi module. Virtual buttons were implemented to allow users to remotely control the main relay and individual load relays through the mobile application. The system status and fault conditions were displayed through indicator widgets which also included notification features to alert users when overcurrent or overvoltage events occurred. The interface design enables secure user access to the system while delivering real-time system updates and smartphone-based remote circuit breaker operation.

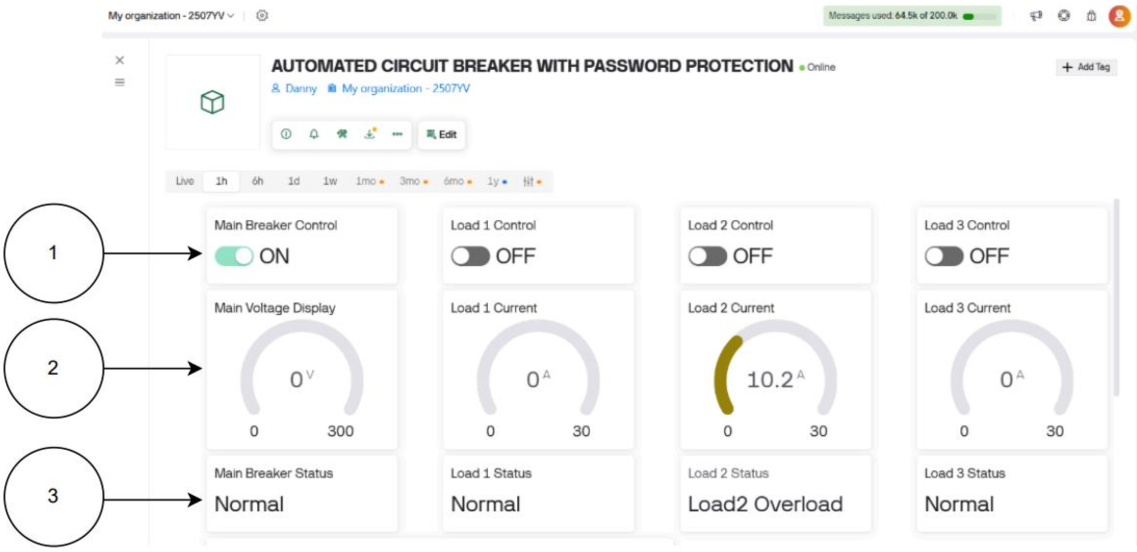



**Fig. 4** *Blynk Interface*

## 4. Result and Discussion

This chapter presented and discussed the results obtained from the development and testing of the IoT-enabled automated circuit breaker system. The system performance evaluation involved functional testing and sensor measurement analysis and fault condition verification during normal and abnormal operating conditions. The results focused on the accuracy of voltage and current sensing, system response during overcurrent and overvoltage events, password-based access control, and remote monitoring and notification using the Blynk application. The discussion interpreted the observed results in relation to the project objectives to evaluate the effectiveness, reliability, and practical applicability of the proposed system for smart home electrical protection.

### 4.1 Prototype Implementation

The prototype of the IoT-Enabled Automated Circuit Breaker demonstrated the physical implementation and integration of the proposed system components. The prototype consisted of an Arduino Mega controller integrated with an ESP8266 Wi-Fi module to enable IoT functionality and remote control. The fundamental protection devices for system loads are Miniature Circuit Breakers (MCBs), but solid-state relays handle automated switching operations. The system provided user access through a keypad interface and an LCD display which showed password verification and system status information. The system used voltage and current sensors to monitor electrical parameters which helped identify faults in the system. The hardware components proved their capability to work in unison through the constructed prototype which delivered both secure access and real-time monitoring along with automatic protection features. Figure 5 shows the prototype of the IoT-Enabled Automated Circuit Breaker developed in this project. The transparent distribution enclosure contained Miniature Circuit Breakers (MCBs) which allowed users to view status indicators directly while providing protection against overcurrent and short-circuit faults. The test and operational phases became easier to manage using labeled switched socket outlets which served as load representations for electrical systems.

**Fig. 5** *Prototype of IoT-Enabled Automated Circuit Breaker*

## 4.2 Circuit Breaker Functional Testing

### 4.2.1 ON/OFF Switching Performance Test

**Table 1** *Result for ON/OFF Switching Performance Test*

| Test No | Load | Command Source | Command Action | Relay Response | Load Status | Switching Delay (s) |
|---|---|---|---|---|---|---|
| 1 | Load 1 | Blynk | ON | Activated | ON | 5.16 |
| 2 | Load 1 | Blynk | OFF | Deactivated | OFF | 2.13 |
| 3 | Load 2 | Blynk | ON | Activated | ON | 2.66 |
| 4 | Load 2 | Blynk | OFF | Deactivated | OFF | 1.61 |
| 5 | Load 3 | Blynk | ON | Activated | ON | 3.27 |
| 6 | Load 3 | Blynk | OFF | Deactivated | OFF | 3.52 |

The smart circuit breaker ON/OFF switching response underwent evaluation through an automated switching performance test which used the Blynk application to control three electrical loads. The loads were controlled from a distance to turn on and off while the time it took for switching was documented. The delay time represented the duration between the command issued from the Blynk application and the corresponding relay action. The results presented in Table 1 indicate that all tested loads responded correctly to both ON and OFF commands, demonstrating reliable relay operation and stable communication between the ESP8266 Wi-Fi module, the Blynk application, and the Arduino controller. Load 1 during testing showed the maximum switching time with an ON/OFF response duration of 5.16 seconds and a switch-off interval of 2.13 seconds. The switching times of Load 2 and Load 3 appeared shorter and more stable when compared to Load 1. The ON commands took longer to respond than the OFF commands because the system needs extra time to process and activate the relay for load activation.

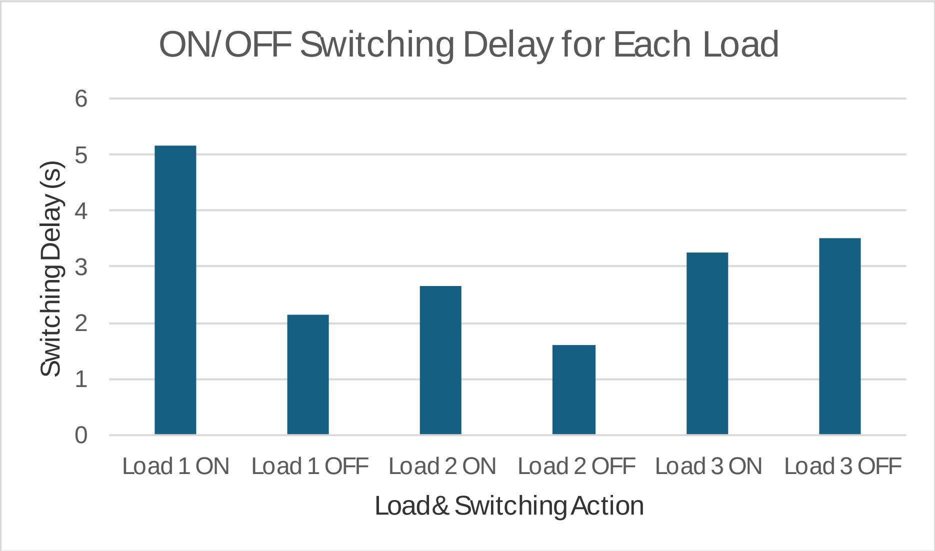



**Fig. 6** *Bar chart for ON/OFF switching delay for each load*

Figure 6 illustrates a bar diagram displaying the time required to switch each load between ON and OFF states. The horizontal axis displays load identification and command actions while the vertical axis represents measured switching delay duration in seconds. The testing data reveals that the ON operation of Load 1 took the most time to complete while Load 2's OFF operation recorded the shortest duration between action and response. The testing data reveals that all OFF operations displayed faster response times than their corresponding ON operations. The system functioned normally because the activation process required the longest time for relay energization and power delivery when compared to the faster load disconnection time. The unique properties of Load 3 interact with the relay's delayed response to higher operating loads resulting in extended switching delays.

### 4.2.2 Authentication Failure Test

**Table 2** *Result for Password Authentication Failure Test*

| Test No | Password Entered | Correct Password | Authentication Result | LCD Message | Wi-Fi Connection |
|---|---|---|---|---|---|
| 1 | 1234 | 1234 | Successful | Access Granted | Allowed |
| 2 | 7896 | 1234 | Failed | Wrong Password | Not Allowed |
| 3 | 2234 | 1234 | Failed | Wrong Password | Not Allowed |
| 4 | 5124 | 1234 | Failed | Wrong Password | Not Allowed |

The authentication testing results as shown in Table 2 evaluated the effectiveness of the password protection mechanism implemented in the smart circuit breaker system. The system allowed access during the first test when the correct password was entered, and the LCD displayed “Access Granted” which enabled remote operation through Wi-Fi connectivity. Users needed to enter incorrect passwords for the authentication tests between tests two and four. The screen showed the message "Wrong Password" after each unsuccessful try and the system blocked all circuit control operations. The test results show that electrical circuits did not operate when users entered invalid credentials during unauthorized access attempts. The system kept the same response which showed that the password-based authentication system worked correctly to block unauthorized access while it made the smart circuit breaker system more secure.

## 4.3 ACS712 Current Monitoring Performance Test

### 4.3.1 Testing of ACS712 for Load 1

**Table 3** *Result of Testing ACS712 for Load 1*

| Injected Current (A) | RMS Voltage (V) | RMS Current (A) | Blynk Current Display (A) | Trip Status |
|---|---|---|---|---|
| 0 | 0.0041 | 0.059 | 0 | Normal |
| 2 | 0.1396 | 2.014 | 2.0 | Normal |
| 4 | 0.2781 | 4.012 | 4.0 | Normal |
| 6 | 0.4072 | 5.875 | 6.0 | Normal |
| 8 | 0.5605 | 8.087 | 8.1 | Normal |
| 10 | 0.6991 | 10.087 | 10.0 | Trip |
| 12 | 0.8348 | 12.045 | 12.0 | Trip |

Table 3 presents the results of Load 1 which show that the ACS712 current sensor operated in a linear and stable manner throughout the current range from 0 to 12 A. The sensor returned when no current flowed produced a 0.0416 V RMS measurement that functioned as the system's zero-current reference. The system demonstrated accurate current detection through the direct proportionality between rising current levels and increased RMS voltage and RMS current values from 2 A to 10 A. The Blynk application presented current data which matched the RMS current readings with an error margin between ±0.1 A to ±0.3 A. The ACS712 sensor maintained its operational levels within the designated ±10% sensitivity boundaries when the Hall-effect sensor with microcontroller ADC conversion yielded standard results. The system worked properly at the normal 0 A to 8 A operating range but detected a “Trip” situation when reaching 10 A which was the Load 1 maximum set limit. The protection system demonstrated its effectiveness by maintaining the trip state throughout the 12 A test. The experimental testing showed that the current measurement system and threshold detection and tripping mechanisms worked properly yet sensor sensitivity and analogue-to-digital conversion caused measurement errors during current processing.

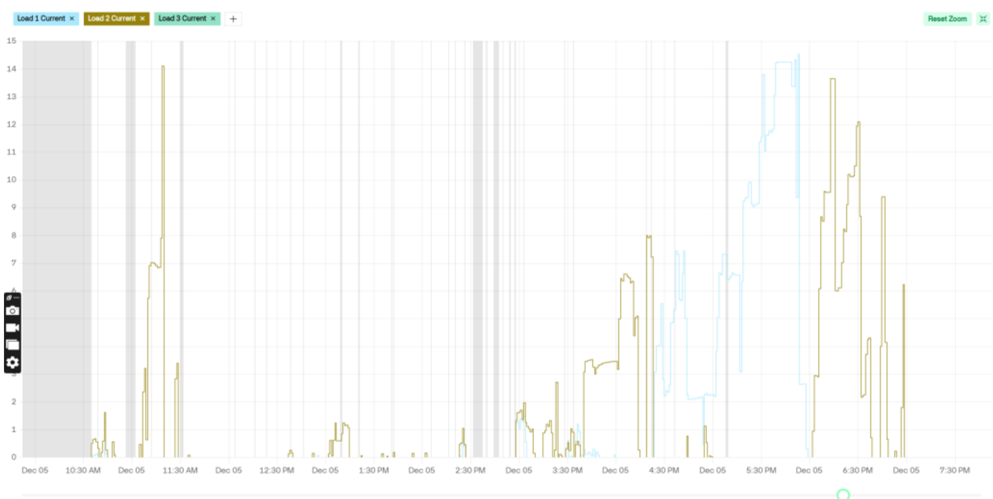



**Fig. 7** *Historical Current Chart on Blynk platform during ACS712 Testing*

Progress in Engineering Application and Technology Vol. 7 No. 1 (2026) p. 267-281

Figure 7 illustrates the current response of Load 1 during step-current injection testing. The blue current plot showed a stable and proportional increase corresponding to each injected current level, confirming the linear response of the ACS712 sensor. The sensor offset along with ADC noise caused the initial readings to fluctuate around zero. The SVERKER 650 operated with accurate voltage-to-current conversion because the plotted current showed exact stepwise increments when the current increased from 2 A to 12 A. The sensor demonstrated stable performance throughout all test points because of its stable plateaus and rising transitions. The system entered a trip condition when the current went above the set limit which showed that the overcurrent detection and protection system worked correctly during testing.

### 4.3.2 Testing of ACS712 for Load 2

**Table 4** *Result of Testing ACS712 for Load 2*

| Injected Current (A) | RMS Voltage (V) | RMS Current (A) | Blynk Current Display (A) | Trip Status |
|---|---|---|---|---|
| 0 | 0.0411 | 0.405 | 0 | Normal |
| 2 | 0.1931 | 1.902 | 2.0 | Normal |
| 4 | 0.4077 | 4.017 | 4.0 | Normal |
| 6 | 0.6172 | 6.082 | 6.1 | Normal |
| 8 | 0.8138 | 8..019 | 8.0 | Normal |
| 10 | 1.0296 | 10.146 | 10.1 | Trip |
| 12 | 1.2286 | 12.107 | 12.1 | Trip |

The results for Load 2, as presented in Table 4, showed that the ACS712 current sensor exhibited stable and linear performance as the injected current increased from 0 A to 12 A. The sensor's baseline showed a minor shift at zero current which resulted from normal sensor noise combined with zero-current drift. The system proved its current detection accuracy through the recorded RMS voltage and RMS current values that matched the injected current range from 2 A to 10 A. The Blynk application displayed current values which matched the RMS current measurements within a range of plus or minus 0.1 to 0.3 A. The sensor tolerance combined with ADC quantization effects produced the observed variations in the system. The normal operating range of Load 2 produced a "Normal" status from 0 A to 8 A, but the device activated a "Trip" condition at 10 A and 12 A because of the overcurrent protection settings. The test results established that Load 2 current measurement and calibration accuracy and overcurrent protection system functioned correctly yet small measurement errors occurred because of the ACS712 sensor properties and digital conversion steps.

### 4.3.3 Testing of ACS712 for Load 3

**Table 5** *Result of Testing ACS712 for Load 3*

| Injected Current (A) | RMS Voltage (V) | RMS Current (A) | Blynk Current Display (A) | Trip Status |
|---|---|---|---|---|
| 0 | 0.0079 | 0.07 | 0 | Normal |
| 5 | 0.3333 | 5.05 | 5.0 | Normal |
| 10 | 0.6768 | 10.25 | 10.2 | Normal |
| 15 | 1.0138 | 15.36 | 15.4 | Normal |
| 20 | 1.3361 | 20.24 | 20.5 | Trip |
| 25 | 1.6634 | 25.20 | 25.5 | Trip |

The results for Load 3, as presented in Table 5, demonstrated that the ACS712 current sensor responded accurately and linearly over a higher current range compared to Load 1 and Load 2. The sensor generated a baseline RMS voltage of 0.0079 V at zero current which represented its typical offset behavior. The sensor maintained its sensitivity during high load operations because the RMS voltage and RMS current values increased proportionally when the injected current went from 5 A to 25 A. The Blynk application shows current values which match the RMS current measurements within acceptable sensor tolerance and ADC conversion limits between ±0.1 A and ±0.3 A. The system kept its "Normal" state between 0 A and 15 A which showed that it detected safe operating conditions correctly, but it switched to "Trip" mode at 20 A and 25 A because of the established overcurrent protection limits. The testing results showed that the current sensing system and ADC processing unit and overcurrent protection system of Load 3 functioned correctly while providing accurate high-range measurements and reliable protection during high load operation.

## 4.4 ZMPT101B Voltage Monitoring Performance Test

**Table 6** *Result of Testing ZMPT101B Voltage Sensor*

| True RMS Voltage (V) | Sensor RMS Voltage (V) | Blynk Display Voltage (V) | Error (%) | Status |
|---|---|---|---|---|
| 0 | 0.0236 | 0 | | Normal |
| 25 | 0.0465 | 33.5 | 34 | Normal |
| 50 | 0.0906 | 55.4 | 10.8 | Normal |
| 75 | 0.1277 | 75.9 | 1.2 | Normal |
| 100 | 0.1666 | 104.8 | 4.8 | Normal |
| 125 | 0.2111 | 125.6 | 0.48 | Normal |
| 150 | 0.2455 | 148.0 | -1.33 | Normal |
| 175 | 0.2908 | 176.1 | 0.63 | Normal |
| 200 | 0.3278 | 198.9 | -0.55 | Normal |
| 225 | 0.3750 | 224.5 | -0.22 | Normal |
| 250 | 0.4130 | 248.6 | -0.56 | Normal |
| 275 | 0.4468 | 267.1 | -2.87 | Trip |

Within ZMPT101B's specified range of 25V to 250V RMS, the device and its conditioning circuit were operating correctly, as shown in the data of Table 6. This data showed that the device gave a generally linear response as the voltage was increased. At zero volts, a small 0.0236V RMS output voltage was recorded due to the internal noise and offset of the sensor, where no measurement of percentage error was made at this point. At low supply voltages of 25V and 50V, measurement errors were relatively high at 34 % and 10.8 % respectively. This was anticipated as low voltage weak sensor output signals are more susceptible to amplifier gain variations, ADC quantization effects and offset noise. Within the range of 75V to 150V, the sensor recorded its greatest accuracy in measurement. The voltage sensor's accuracy was consistently in a range of 1.33% to 1.20%. This indicates that the sensor maintains its reliability and stability in measuring voltages. The device was still functioning linearly in the range of 175V to 250V with an error of -0.22% to -0.56%. Between 0 and 250V the smart circuit breaker remained in a normal operating state, tripping to 275V to confirm the correct functioning of the voltage detection and over voltage protection logic. Under normal mains voltage conditions, the ZMPT101B accurately measures voltage, however, it tends to underestimate at very low voltage levels due to resolution issues inherent in its design.

Progress in Engineering Application and Technology Vol. 7 No. 1 (2026) p. 267-281

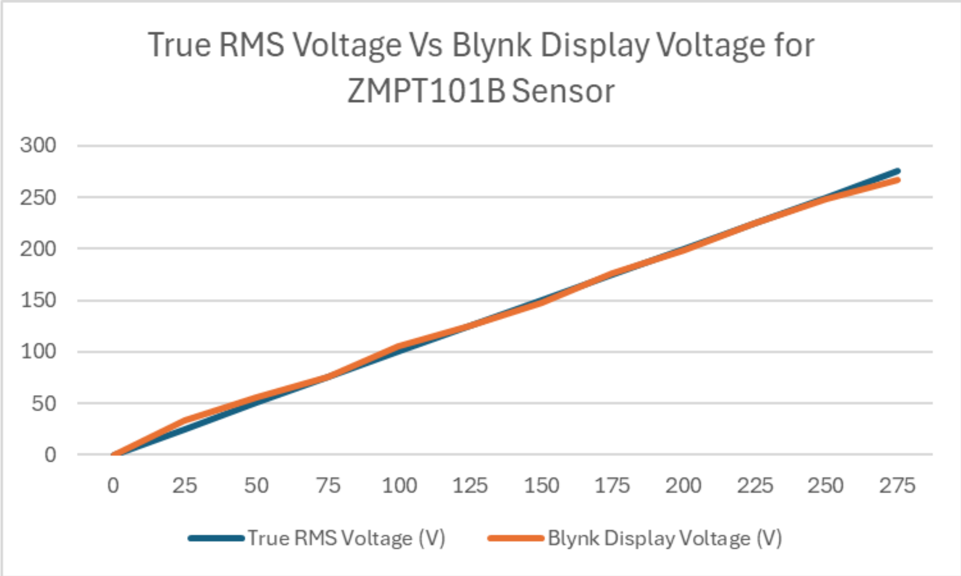



**Fig. 8** *Comparison of True RMS Voltage and Blynk Display Voltage for the ZMPT101B Sensor*

As shown in Figure 8, the measured voltage of the ZMPT101B voltage sensor and the Blynk application have a good linear relationship, thus the measured voltage of the ZMPT101B voltage sensor can be used to display the True RMS voltage on Blynk. Across the whole range of voltages tested, the two curves show a straight-line relationship with a consistent trend. At low voltage, the Blynk display read slightly higher values because weak sensor signals were more prone to noise and ADC quantisation effects, which resulted in larger percentage errors. At voltages more than 75V, the reading the multimeter gave for true RMS was very close to the true RMS voltage reading, which indicates better precision and stability. The ZMPT101B voltage sensor provided a reliable and direct voltage reading over the 75V to 250V range with a slight loss of accuracy at the lowest voltage.

## 4.5 Notification Failure Test

**Table 7** *Result for Notification Failure Test*

| Test Condition | Wi-Fi Status | LCD Message | Blynk Status | Notification Status | Circuit Protection |
|---|---|---|---|---|---|
| Normal Operation | Connected | Load 1 Overload | Updated | Sent | Active |
| Wi-Fi Disconnected | Disconnected | Wi-Fi Failed | Not Updated | Not Sent | Active |
| Overcurrent during Wi-Fi failure | Disconnected | Wi-Fi Failed | Not Updated | Not Sent | Relay Tripped |

The testing of failure notifications, shown in Table 7, checked how the system behaved normally, when disconnected from the Wi-Fi network, and when there was overcurrent during Wi-Fi failure. The system in normal operation maintained a stable wireless internet connection and displayed a message on the LCD about an overload. Additionally, it updated in real time the Blynk app and sent notifications to users. On disconnection of Wi-Fi, the LCD displayed a "Wi-Fi Failed" message on the screen, followed by the Blynk platform that failed to update and no notifications were received. The system was operational in its data acquisition and processing functions, even if connectivity had been broken. In the absence of a Wi-Fi connection the relay successfully disconnected the load from the power supply when the current rose to a level greater than its set limit. Safety is always ensured through the independent operation of protection logic irrespective of network availability, thus notification and remote monitoring functions failing do not compromise electrical safety.

## 5. Conclusion

The project was to develop an automated circuit breaker using the technology of IoT for smart home. The automated circuit breaker has a password protection feature. A microcontroller based industrial control system has been designed with the aid of a keypad, LCD display and relay modules for the purposes of user interaction, status display and actuation of devices respectively. The system also incorporates voltage and current sensors.

The data gathered from the experiment indicated that the system functioned properly in relation to the monitoring of electrical properties and promptly isolated the power in response to irregularities. In normal working conditions, the system provided vital alerts to the users. The password system stopped unauthorized users from accessing the device and the physical locking mechanism continued to work in the event of a Wi-Fi disconnection, also always ensuring electrical safety.

The project was successful in its aims by developing an automatic circuit breaker system utilizing IoT technology to offer homeowners real time monitoring and remote control of their homes via the internet. This protection system safeguards against electrical overvoltage and overcurrent. Access to the system is protected by a user ID and password combination. This adds a level of security for those users who have been given permission to use the system. Further research could involve the development of more accurate measurement of the low voltage which is involved in the smart plug. Additionally, smart plugs should be designed to include protection against hacking, also their capabilities should be extendable to be used in a variety of homes and businesses.

## Acknowledgement

The authors wish to extend their gratitude to the Department of Electrical Engineering Technology of the Faculty of Engineering Technology, Universiti Tun Hussein Onn Malaysia for the facilities and support provided. This was during the completion of the project "IoT-Enabled Automated Smart Circuit Breaker with Password Protection for Smart Homes using Arduino and ESP8266". The faculty provided the proposed system's developers with significant assistance in the form of technical advice, laboratory facilities and access to equipment.

## References

[1] Sahabudin, N. F. A., Rusli, J. R., Ahmad, I., Kahar, N. H. A., Azmi, M. a. M., & Roslan, N. F. (2024). Development of a Real-Time Electrical Monitoring System for Residential Buildings. *2024 IEEE 10th International Conference on Smart Instrumentation, Measurement and Applications (ICSIMA)*, pp.224–228. https://doi.org/10.1109/icsima62563.2024.10675545

[2] Varade, K., Mhatre, O., Vartak, G., & Singh, D. (2021). Smart Circuit Breaker using IoT Technology. *International Research Journal of Engineering and Technology (IRJET)*, *8*(11), pp. 702–705.

[3] Kumar, V. A., Nandalal, V., Sheikdavood, K., & Kumaresan, S. J. (2022). Smart Application Based Circuit Breaker with Secure Passcode. *2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC),* pp. 1–5. https://doi.org/10.1109/icmnwc56175.2022.10031851

[4] Kalaimani, I., Dhivya Dharshini, Dinesh, & Navaneethan. (2023). IoT Based Circuit Breaker Controller. *2023 International Conference on Sustainable Emerging Innovations in Engineering and Technology (ICSEIET),* pp. 144–149. https://doi.org/10.1109/icseiet58677.2023.10303602

[5] Srivathsan, R., Logesh, S. J., Kavitha, D. (2022). GSM and Arduino Based Smart Circuit Breaker. *2022 1st International Conference on Computational Science and Technology (ICCST)*, pp.67–70. https://doi.org/10.1109/iccst55948.2022.10040273

[6] Yadav, A., & Sharma, V. K. (2023). Smart MCB Design using Embedded and IOT system. *2022 International Conference on Computer Communication and Informatics (ICCCI)*, pp.1–6. https://doi.org/10.1109/iccci56745.2023.10128488

[7] Siregar, Y., & Tandry, E. (2023). Monitoring System Design and Controlling Smart Home Features with The Blynk App. *2023 7th International Conference on Electrical, Telecommunication and Computer Engineering (ELTICOM),* pp. 139–143. https://doi.org/10.1109/elticom61905.2023.10443083