iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.77489

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

Secure Smart Meter for Real-Time Usage Tracking and Anti-Theft Control

Bibin Rajan[1], Sanju Anna Kurien[2], Amar M Haneefa[3], Sidhu Madhav S[4], Prof. Arya Lekshmi V[5], Prof. Anu George[6]
Department of Electrical and Electronics Engineering Mar Athanasius College of Engineering, Kothamangalam, Kerala

Abstract: ***The Secure Smart Meter for Real-Time Usage Tracking and Anti-Theft Control is designed to address a major challenge in the power sector—electricity theft. The system enables accurate and real-time monitoring of energy consumption while detecting unauthorized usage. Built around the ESP32 microcontroller, the meter uses multiple PZEM-004T energy measurement modules to measure voltage, current, power, and energy at different points in the supply line. Electricity theft is detected by comparing the measured values of the modules, where any significant mismatch indicates illegal power tapping or bypassing. Upon detection of abnormal conditions, the system automatically disconnects the supply using a relay mechanism to prevent further losses. The measured energy parameters and theft status are displayed in real time on a website, providing remote monitoring and transparency. This IoT-based solution is cost-effective, scalable, and offers a smarter alternative to conventional energy meters.***

Keywords: Smart Meter, Electricity Theft Detection, IoT, ESP32, PZEM-004T, Real-Time Monitoring

I. INTRODUCTION

The global energy sector is essential for facilitating contemporary technological and economic advancement. Nevertheless, the issue of electricity theft poses a significant challenge for power distribution networks, resulting in financial setbacks for utility companies and impacting grid stability. In numerous developing nations, this leads to power losses, voltage irregularities, and equipment overloads. To tackle this problem, modern energy management systems incorporate Internet of Things (IoT) and embedded technologies for effective monitoring. IoT-enabled smart meters facilitate real-time data collection and communication between consumers and utility providers. By utilizing sensors, microcontrollers, and cloud platforms, these systems can track electrical parameters such as voltage, current, and power via web or mobile interfaces. The proposed initiative, Secure Smart Energy Meter for Real-Time Usage Tracking and Anti-Theft Control, employs an ESP32 microcontroller along with PZEM-004T energy monitoring modules to assess electrical parameters on both the supply and load sides. The system consistently compares these measurements to identify any abnormal discrepancies that may suggest electricity theft. Upon detecting a mismatch, the system triggers an alert and has the capability to disconnect the load using a relay. Additionally, the data is transmitted to a web-based platform for real-time monitoring, offering a cost-effective and dependable solution to mitigate electricity theft and enhance power distribution efficiency.

II. PROPOSED SYSTEM

The proposed system introduces a Secure Smart Meter that facilitates real-time monitoring, data logging, and the detection of electricity theft through an IoT-based platform. This system aims to enhance transparency in energy consumption and ensure precise monitoring of power usage within distribution networks. The system employs PZEM-004T energy monitoring modules to assess electrical parameters such as voltage, current, power, and energy consumption from both the grid and the load sides. These modules deliver real-time measurements, which are relayed to the ESP32 microcontroller. The ESP32 serves as the central processing unit, tasked with collecting, analyzing, and transmitting the measured data.

The ESP32 consistently compares the readings from the supply side with those from the load side. Under standard conditions, the power supplied by the grid and the power consumed by the load should be nearly equivalent, barring minor technical losses. Should the system identify a significant discrepancy between these values, it may suggest electricity theft or unauthorized tapping in the supply line.To facilitate remote monitoring, the ESP32 transmits the gathered data to a cloud-based web dashboard, enabling users and utility providers to monitor real-time energy consumption. Furthermore, the system incorporates a relay mechanism that can automatically disconnect the load when theft or abnormal conditions are detected. This system enhances billing accuracy, promotes transparency, and supports effective energy management.

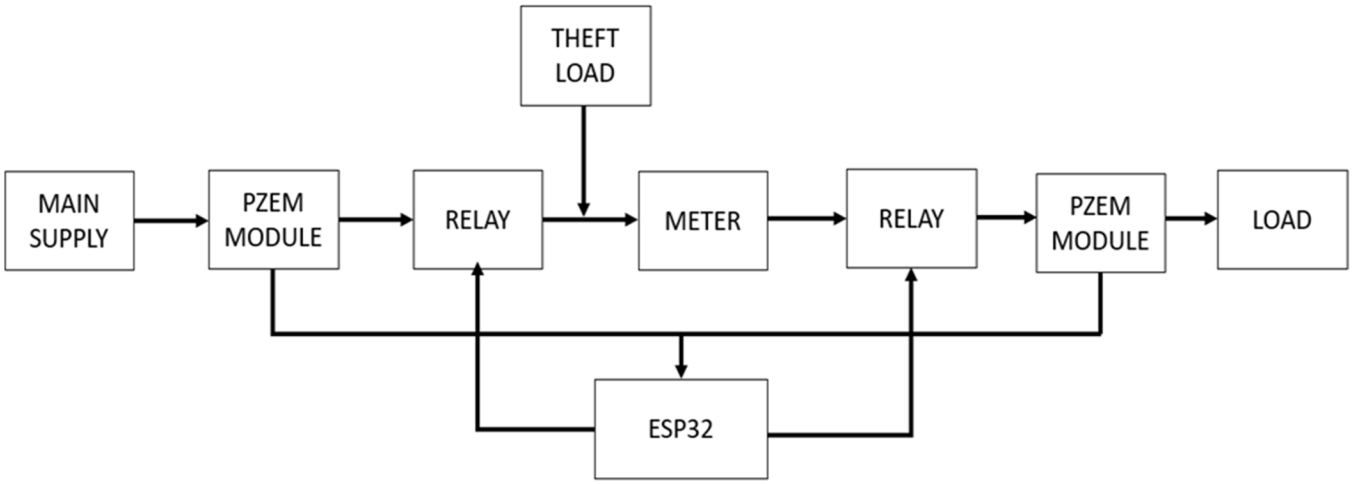


Fig. 1 Block Diagram of Smart Meter

A. Energy Measurement and Data Acquisition

The proposed system utilizes two PZEM-004T energy monitoring modules to measure electrical parameters at various points along the distribution line. As depicted in Fig. 1: Smart Energy Meter System Architecture, the grid supply serves as the primary source of electrical power delivered by the utility to the consumer's premises. The first PZEM-004T module is installed on the grid side to monitor voltage, current, power, and energy entering the system. These measurements reflect the total electrical energy provided by the utility. The second PZEM-004T module, also shown in Fig. 1, is located on the load side, following the main energy meter. It records the electrical parameters consumed by the authorized loads. Under standard operating conditions, the energy measured on both the grid side and the load side should be nearly identical, barring minor transmission losses. However, if an unauthorized connection or theft load is tapped before the meter, a portion of the electricity will be consumed without being recorded, resulting in a significant discrepancy between the two measurements. The data collected from both modules is sent to the ESP32 microcontroller, which continuously gathers and processes the electrical parameters. By analyzing the readings from both the grid side and load side, the system is capable of identifying abnormal variations that may suggest electricity theft.

B. IoT Monitoring, Theft Detection, and Control System

The proposed system utilizes two PZEM-004T energy monitoring modules to measure electrical parameters at various points along the distribution line. As depicted in Fig. 1: Smart Energy Meter System Architecture, the grid supply serves as the primary source of electrical power delivered by the utility to the consumer's premises. The first PZEM-004T module is installed on the grid side to monitor voltage, current, power, and energy entering the system. These measurements reflect the total electrical energy provided by the utility. The second PZEM-004T module, also shown in Fig. 1, is located on the load side, following the main energy meter. It records the electrical parameters consumed by the authorized loads. Under standard operating conditions, the energy measured on both the grid side and the load side should be nearly identical, barring minor transmission losses. However, if an unauthorized connection or theft load is tapped before the meter, a portion of the electricity will be consumed without being recorded, resulting in a significant discrepancy between the two measurements. The data collected from both modules is sent to the ESP32 microcontroller, which continuously gathers and processes the electrical parameters. By analyzing the readings from both the grid side and load side, the system is capable of identifying abnormal variations that may suggest electricity theft.

The operational framework of the electricity theft detection system is depicted in Fig. 2. The procedure initiates with the measurement of electrical parameters, including voltage, current, and power, at two distinct points along the distribution line. The grid-side power signifies the total energy provided by the utility, whereas the load-side power indicates the actual energy utilized by the authorized load. These parameters are assessed using PZEM-004T energy monitoring modules. The collected data is transmitted to the ESP32 microcontroller, which persistently observes and evaluates the readings. The ESP32 juxtaposes the grid-side and load-side power values to ascertain whether the system is functioning normally. In standard conditions, both values remain nearly equivalent, aside from minor technical losses in the line.

Should the grid-side power significantly exceed the load-side power, it suggests potential electricity theft or unauthorized tapping within the supply line. When this situation arises, the system recognizes it as theft detected and generates an alert to inform the monitoring platform. If no irregular difference is detected, the system maintains normal operations and continues to monitor the system consistently

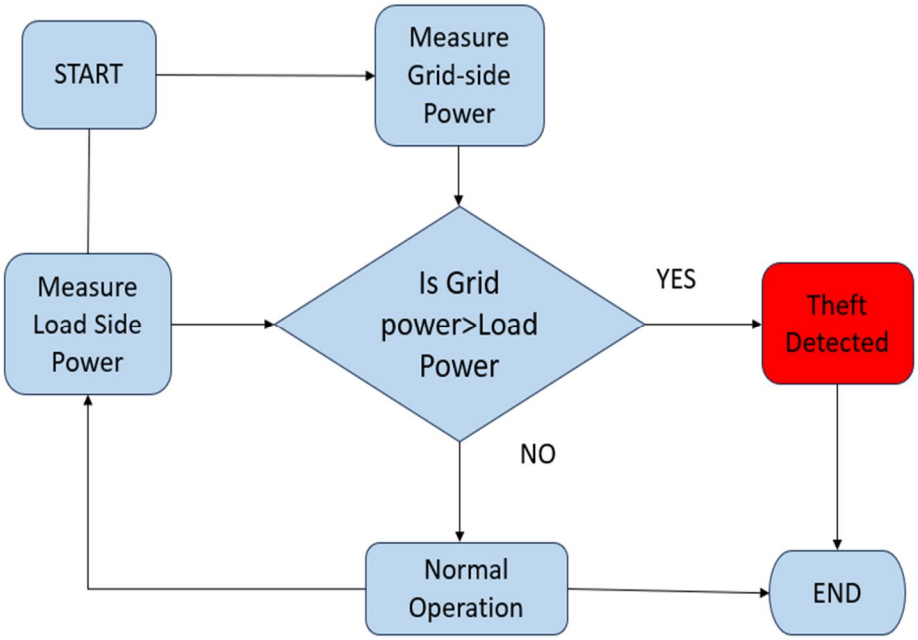


Fig. 2 Working Flow of the Smart Meter System

III.SIMULATION AND RESULTS

The proposed Secure Smart Energy Meter for Real-Time Usage Tracking and Anti-Theft Control was validated through simulation before hardware implementation. The simulation was performed using the Proteus Design Suite, which provides a virtual platform for testing embedded systems and electronic circuits. The simulated model includes essential components such as the Arduino Uno microcontroller, ACS712 current sensors, relay module, LCD display, indicator LEDs, and load elements. The purpose of the simulation was to verify the system's ability to monitor energy consumption and detect electricity theft by comparing the current values measured at the supply side and load side. The microcontroller continuously receives analog signals from the current sensors and processes them to determine the operating condition of the system. If the difference between the measured currents exceeds a predefined threshold, the controller identifies the situation as an abnormal condition indicating possible electricity theft. The simulation setup replicates real-world operating conditions and validates the sensing accuracy, control logic, and response capability of the system before practical implementation.

A. System Operating Conditions

The performance of the proposed Secure Smart Meter was evaluated under different operating conditions to verify the accuracy of sensing, system stability, and the effectiveness of the detection algorithm. The system behavior was analyzed in both off-state and normal operating conditions before testing the theft detection mechanism.

In the off condition, the circuit remains inactive with no load connected to the system. Under this state, the current flow through the circuit is minimal and the sensors do not detect any significant electrical activity. The relay remains in an open state, preventing power delivery to the load. The LCD display also remains inactive, indicating that the system is not monitoring any energy consumption. This condition verifies that the system remains stable when no electrical load is connected and confirms that the controller does not generate false readings or trigger unnecessary alerts. The simulation corresponding to this state is shown in Figure 3.

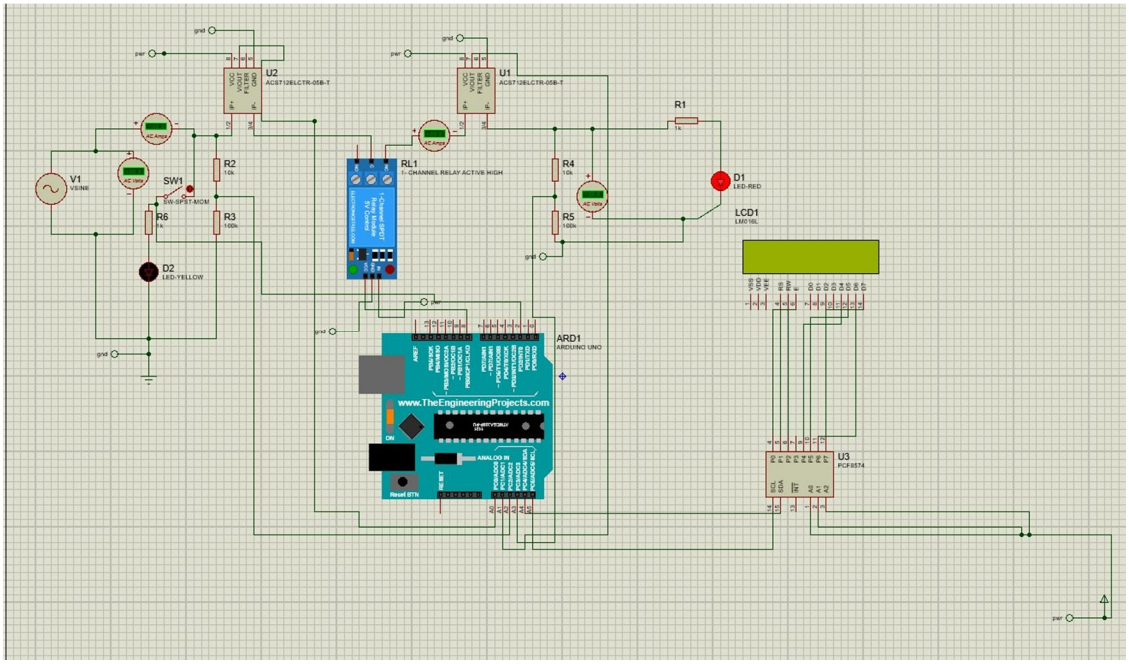


Fig. 3 Simulation of off condition

When the authorized load is connected, the system enters the normal operating condition. In this state, the current measured at the grid-side sensor and the load-side sensor remains nearly identical because all supplied energy passes through the legal metering path before reaching the load. The microcontroller continuously compares these sensor readings and confirms that the difference between them remains within the predefined threshold limit. Since no abnormal deviation is detected, the controller classifies the system state as normal operation.

During this condition, the relay remains energized to allow uninterrupted power supply to the authorized load. The green indicator LED turns on to visually indicate normal system operation, while the LCD display shows the status message “NORMAL” along with the measured current values. This stage of the simulation verifies that the sensing mechanism, comparison algorithm, and control logic operate correctly without producing false alarms during legitimate energy consumption. The Proteus simulation of this condition is illustrated in Figure 4.

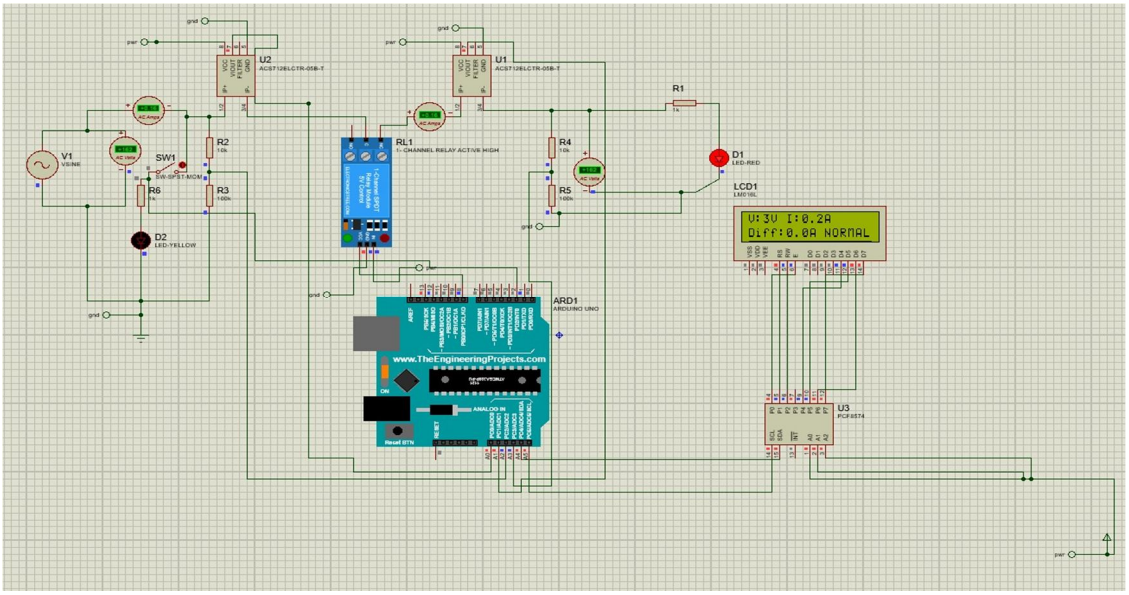


Fig. 5 Simulation of normal Condition

B. Simulation of Electricity Theft Condition

To evaluate the effectiveness of the proposed anti-theft mechanism, an electricity theft condition was introduced in the simulation environment. This was achieved by connecting an additional unauthorized load before the metering point, thereby allowing a portion of the supply current to bypass the legal energy meter. As a result, the grid-side current measured by the first sensor becomes higher than the load-side current measured by the second sensor.

The microcontroller continuously compares these two sensor readings and identifies a significant discrepancy between them. When the difference exceeds the predefined threshold value, the system interprets this condition as electricity theft. Immediately after detecting the anomaly, the controller executes a protection action by sending a signal to deactivate the relay. This action disconnects the load from the supply line, thereby preventing further unauthorized energy consumption.

At the same time, the LCD display updates its message to "THEFT DETECTED," providing immediate visual confirmation of the abnormal condition. The red indicator LED turns on while the green LED turns off, clearly indicating that the system has identified a theft event and interrupted the power supply. The rapid transition between normal operation and theft detection demonstrates the responsiveness and reliability of the detection mechanism. The simulation result corresponding to this condition is illustrated in Figure 5.

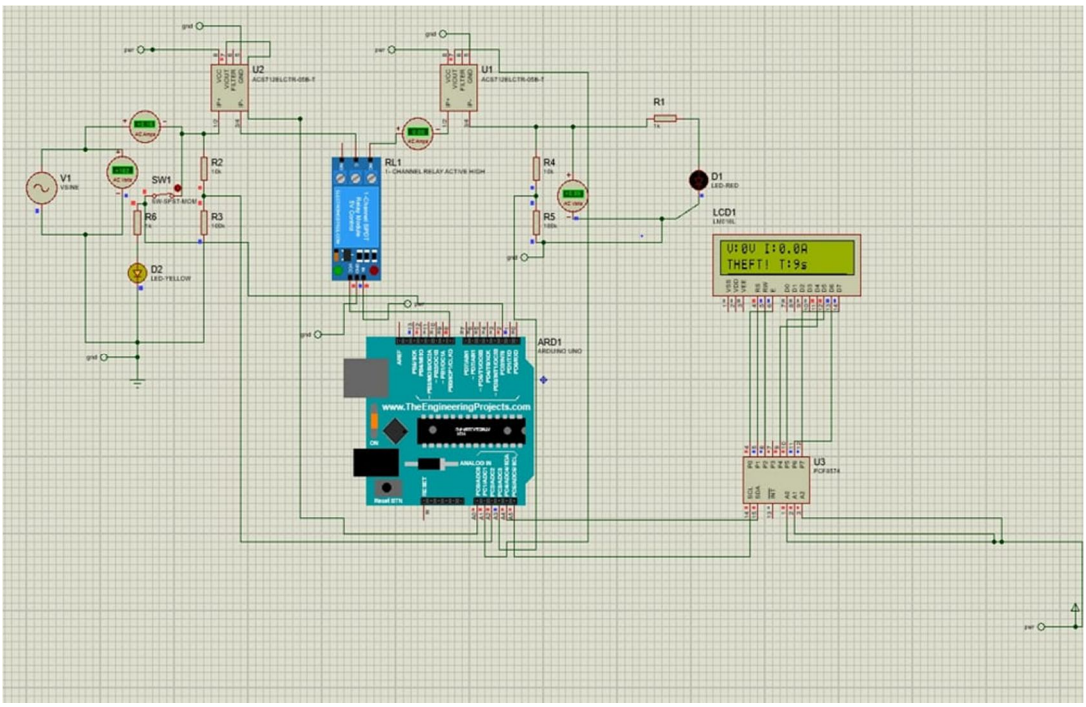


Fig. 5 Simulation of Theft condition

C. Data Monitoring and IoT Interface

The In addition to local monitoring, the system supports real-time data acquisition and remote monitoring through an IoT-enabled platform. Electrical parameters such as voltage and current are continuously measured and transmitted to a cloud-based monitoring interface through wireless communication. This interface allows users and utility providers to observe energy consumption in real time and analyze usage patterns effectively. The monitoring platform displays real-time electrical data and system status updates, ensuring that any irregularities in energy consumption can be identified immediately. The integration of IoT technology enhances system transparency and enables remote supervision of electricity usage, making the system suitable for modern smart grid applications.

D. Performance Evaluation

The simulation results demonstrate that the proposed smart meter operates reliably under different operating conditions. The sensors accurately measure electrical parameters and the controller successfully detects discrepancies between the supply and load currents. The relay-based protection mechanism responds immediately to theft detection, ensuring rapid isolation of the load from the supply.

Furthermore, the LCD display and indicator LEDs provide clear visual feedback regarding the system status, enabling users to easily identify normal operation or theft conditions. The consistency of the simulation results across multiple trials confirms the reliability of the detection algorithm and the overall stability of the system.

IV. HARDWARE IMPLEMENTATION

The hardware setup of the Secure Smart Meter is designed to monitor electrical parameters and detect electricity theft in real time. The complete circuit diagram of hardware prototype is shown in Figure 6.

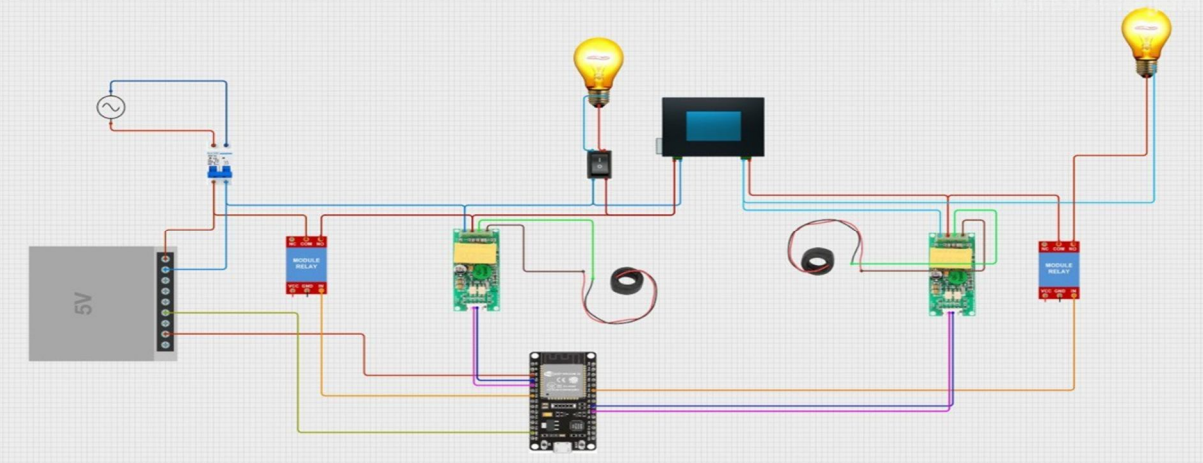


Fig. 6 circuit diagram for hardware prototype.

The AC supply from the grid is first connected through a Miniature Circuit Breaker (MCB), which provides protection against overloads and short circuits. After the MCB, the supply line is connected to the sensing and measurement units of the system.Two PZEM-004T energy monitoring modules are used to measure important electrical parameters such as voltage, current, power, and energy consumption on both the supply side and the load side. Each module uses a CT sensor to measure the current flowing through the respective line. The measured data is transmitted to the ESP32 microcontroller, which acts as the main processing unit of the system.The ESP32 continuously receives data from both PZEM modules and compares the supply-side and load-side readings. Under normal conditions, both values remain nearly equal. If a significant difference is detected, it indicates possible electricity theft or unauthorized tapping in the supply line. The ESP32 then sends the data to a web-based monitoring platform for real-time observation and can also generate alerts.

The system also includes relay modules that act as electrically controlled switches. These relays are connected to the ESP32 and can disconnect the load automatically when theft or abnormal conditions are detected. This hardware configuration ensures accurate measurement, continuous monitoring, and quick detection of electricity theft. The complete hardware prototype is shown in Figure 7.

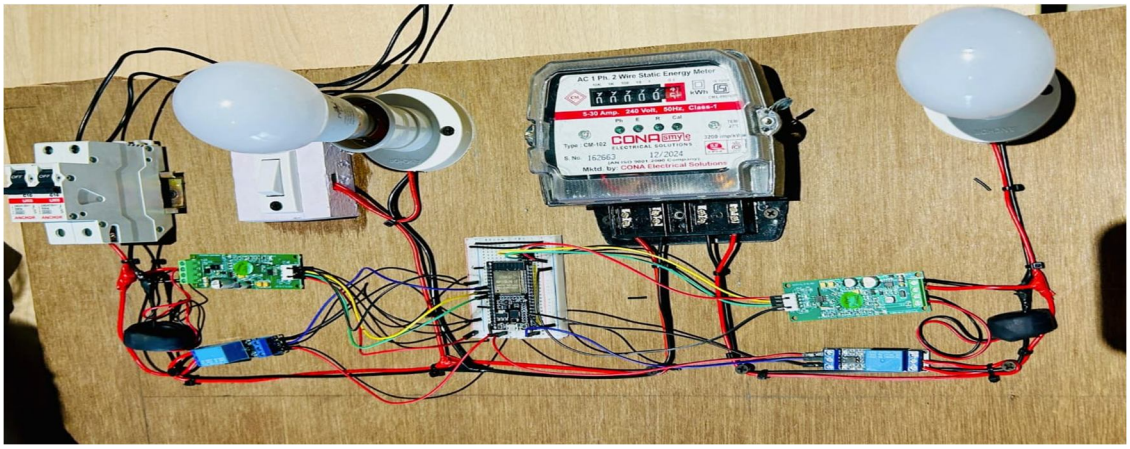


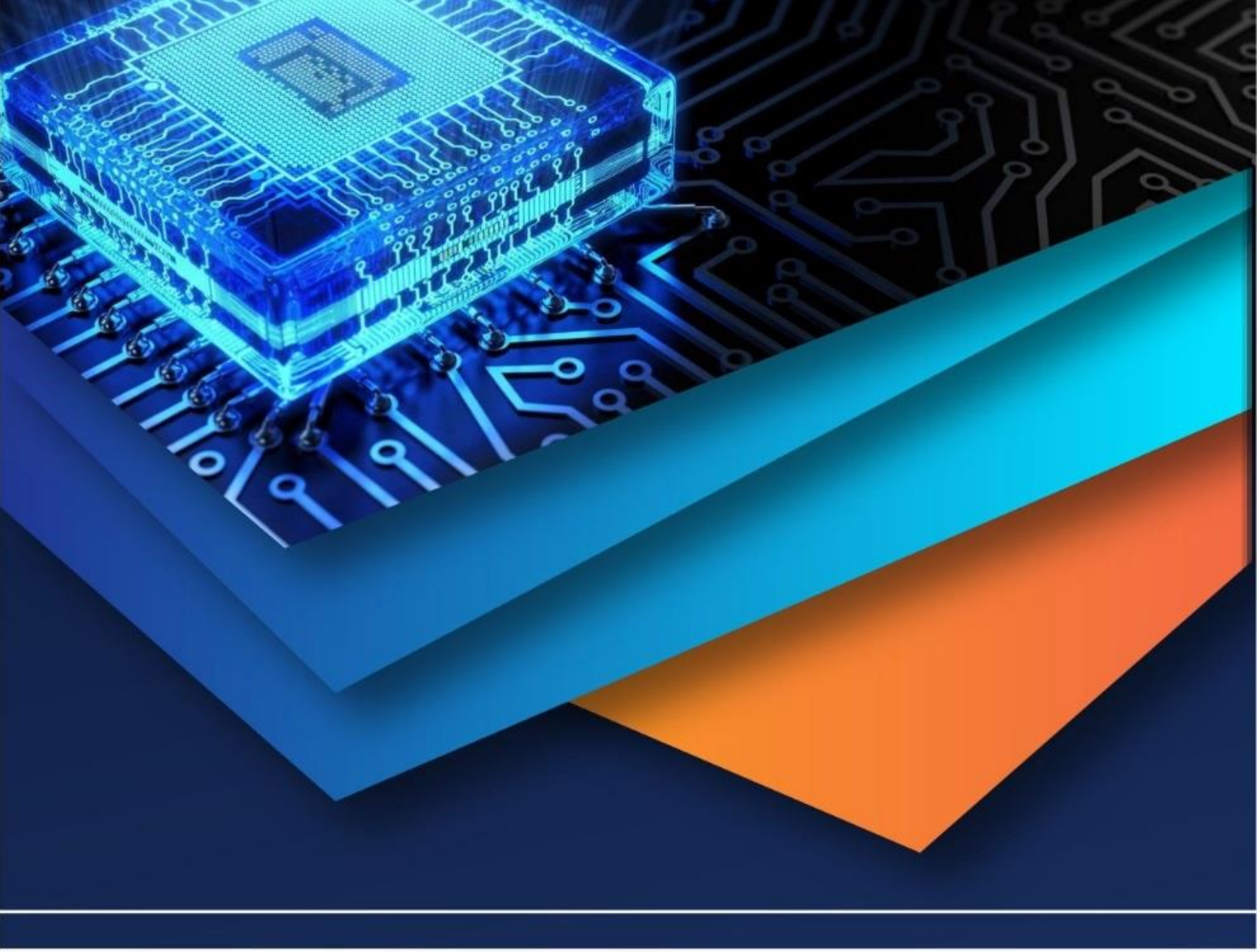
Fig. 8 Hardware Prototype of Smart Meter System

V. CONCLUSION

The proposed Secure Smart Meter provides a comprehensive solution for real-time energy monitoring and automatic electricity theft detection. By integrating voltage and current sensors with the ESP32 microcontroller, the system continuously measures energy consumption at both supply and consumer ends, ensuring accurate detection of discrepancies that may indicate theft. The use of a relay module allows immediate load disconnection in case of unauthorized usage, while the LCD display and web interface enable real-time alerts and remote monitoring. The hardware design is low-cost, scalable, and reliable, making it suitable for residential, commercial, and smart grid applications. Its dual-mode monitoring, combining local display and cloud-based dashboards, enhances user awareness and utility management capabilities. Overall, this system not only improves energy accountability but also contributes to energy conservation and efficient power distribution. Future work could involve integrating machine learning algorithms for predictive theft detection, energy forecasting, and advanced data analytics to further enhance grid intelligence.

REFERENCES

[1] M. U. Saleem, M. R. Usman, and M. Shakir, "Design, implementation, and deployment of an IoT based smart energy management system," *IEEE Access*, vol. 9, pp. 59649–59664, 2021.
[2] R. S. Gaikwad, "IoT based smart meter using ESP32," *International Journal of Research Publication and Reviews*, vol. 5, no. 5, pp. 2360–2370, 2024.
[3] Y. Siregar and Y. R. P. Manurung, "Smart energy meter design with notifications and over-electric energy consumption cut-off with ESP32 MCU node using the Blynk IoT application," 2023.
[4] B. Jyothi, C. Gompa, C. Vajrapu, R. Matchetti, A. Yadla, J. S. G. Kaki, and S. S. Putcha, "A smart energy meter using IoT for monitoring and control energy via web application," in *2023 IEEE Renewable Energy and Sustainable E-Mobility Conference (RESEM)*, IEEE, 2023.
[5] M. Muhammad, A. Ahmed, O. Zeyad, E. Amr, M. Ahmed, H. Abdelrahman, and M. Aboelela, "IoT-based smart meter with energy theft detection," in *2023 IEEE International Conference on Smart Applications, Communications and Networking (SmartNets)*, pp. 111–114, IEEE, 2023.
[6] M. Alam and R. Anwar, "Power theft detection using smart meter and IoT," in *IEEE Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES)*, pp. 1–5, IEEE, 2020.
[7] B. K. Barman, S. N. Yadav, S. Kumar, and S. Gope, "IoT based smart energy meter for efficient energy utilization in smart grid," 2018.
[8] K. H. D. P. Kumar and W. D. V. S. Tharuka, "Detection of electricity theft in smart grid using IoT," in *2020 IEEE International Conference on Electrical, Computer and Communication Engineering (ECCE)*, pp. 1–6, IEEE, 2020.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY