ELECTRICITY MONITORING AND PREVENTION SYSTEM WITH ANTI-THEFT BY USING IOT-BASED TECHNOLOGY

Dheiven Kyle D. Estabillo, John Russel A. Guevarra, John Dominic G. James, JV Dominic D. Pilar, Wenson R. Evangelista, REE

ABSTRACT

This paper presents the development and performance evaluation of an IoT-based Electricity Monitoring and Prevention System with Anti-Theft capability**,** designed to address power losses caused by unauthorized energy usage. The system employed an ESP-WROOM32 microcontroller, interfaced with PZEM-004T energy sensors, and used the ZigBee communication protocol for wireless data transmission. Real-time voltage, current, and power readings were obtained and visualized through the Blynk application, enabling remote monitoring and control. System validation involved comparative testing of measured and reference values obtained from calibrated instruments, with percent error computed and t-tests applied. The results indicated percent errors ranging from 0.53% to 1.72%, demonstrating high measurement precision and reliability. The anti-theft detection mechanism exhibited 100% sensitivity, specificity, and success rate in identifying abnormal consumption patterns. Cost-benefit analysis confirmed economic feasibility with a positive net benefit beyond a 3.94% theft probability threshold. Overall, the proposed system demonstrates robustness, scalability, and the potential to be integrated into modern smart grid infrastructure to enhance energy monitoring accuracy and prevent energy theft.

Keywords: IoT-based energy monitoring, electricity theft prevention, ESP-WROOM32, ZigBee communication, PZEM-004T sensor, smart grid, real-time data acquisition

INTRODUCTION

One solution to energy theft by utilities involves relocating electric meters to elevated metering centers, away from residential buildings. The length of the service conductors had made them vulnerable to illegal connections. The proposed solution is a system with mechanisms for theft recognition and magnitude determination. The two mechanisms work based on voltage and energy readings. The system was designed and tested using a residential building-rated microcontroller-based prototype utilizing an energy monitor as an input device and the ZigBee protocol for wireless communication. The sensitivity, specificity, and recognition success rate were all 100 percent. The percent error of the theft magnitude determination mechanism ranged from 0 to 2.17 percent. Through cost-benefit analysis, the system was found to have a positive net benefit at theft probabilities higher than 3.94 percent. The system has excellent usability as assessed through the System Usability Scale (Andaya et al., 2018).

The electric meter examines the implementation, advantages, and challenges of smart meters, which provide real-time electricity usage data and enable two-way communication between consumers and utility providers. Notable benefits include precise billing, enhanced energy efficiency, theft detection, and improved grid management. The study emphasizes the effects of smart meters on consumption behavior, customer satisfaction, and the reduction of electricity theft. Electric meters enable consumers to respond to dynamic pricing signals from utilities, adjusting their energy consumption during peak hours or when prices are high. The paper highlights that smart meters are essential for real-time communication between utilities and consumers, enabling flexible energy consumption patterns. This flexibility is key to reducing

strain on the grid during high-demand periods and ensuring a more balanced energy supply (Siano, P. 2016).

According to Sharma et al. (2016), integrating IoT technology with smart meters improves energy efficiency and reduces waste. IoT-based smart meters enable real-time monitoring of electricity consumption, providing consumers with immediate feedback on their usage patterns. This feedback helps users make more informed decisions about when and how much electricity to use, reducing their energy bills and overall consumption. Additionally, the paper touches on the role of smart meters in detecting abnormal consumption patterns, which may indicate theft or technical issues within the grid.

In the study of Madhu G M et al. (2020), an IoT-enabled smart metering system was used to monitor and prevent electricity theft. Their system integrates sensors and microcontrollers that continuously monitor energy flow and compare actual consumption with recorded data. If there's any tampering with the meter or an unusual surge in energy use that suggests theft (such as bypassing or tapping the electricity), the system flags the behavior. The IoT aspect enables the system to send real-time data to a cloud server, where analytics algorithms can detect anomalies. This provides an advantage over traditional meters, which are more vulnerable to tampering because they lack a real-time detection mechanism. By leveraging the cloud, utilities or authorities can monitor multiple locations remotely, receive instant notifications about potential theft, and respond promptly.

Mtair et al. (2024) presented a comprehensive overview of an IoT-based energy meter using the ESP32 to monitor energy consumption and detect theft. The algorithms used for anomaly detection highlight the importance of identifying unusual consumption patterns. Exploring the design and implementation of a user-friendly interface allows consumers and utility managers to monitor usage remotely. The authors conclude that their solution effectively mitigates electricity theft, thus reducing economic losses for utility companies.

Utilizing an Arduino microcontroller, the system collects energy usage data. It transmits it via Wi-Fi to a central server, enabling remote monitoring and management. Additionally, the GSM module facilitates alert notifications in the event of abnormal activities, suggesting potential energy theft. The implementation of this system promises to significantly reduce manual intervention, improve energy monitoring accuracy, and strengthen measures against unauthorized energy use, thereby contributing to more reliable and secure energy management. Through detailed experimental validation, the system's effectiveness and practicality are demonstrated, showcasing its potential for widespread adoption in modern energy infrastructure. (Birajdar et al., 2024).

This study aimed to design an IoT-based electricity monitoring and theft-prevention system that enables real-time tracking and enhances protection against unauthorized electricity use. Specifically, the study sought to design a system capable of real-time electricity monitoring and theft prevention using IoT technology. It also aimed to develop and implement a functional prototype of the proposed system. Furthermore, the prototype was tested to evaluate its performance and effectiveness, with the goal of generating insights that can guide future improvements and research in this field.

Conceptual Framework

Figure 1

Conceptual Framework

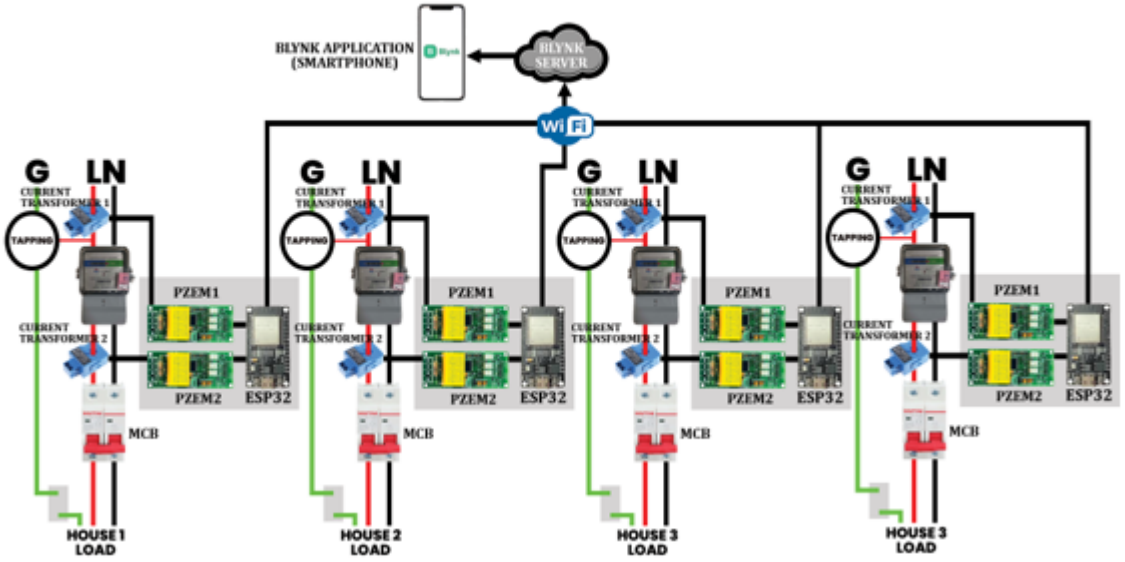
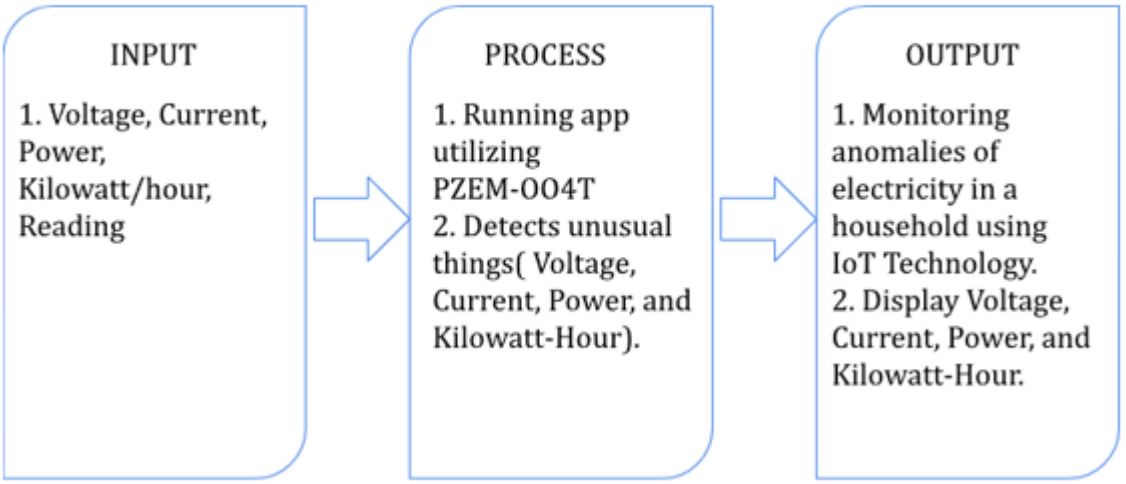


Figure 2

Input, process, and input diagram



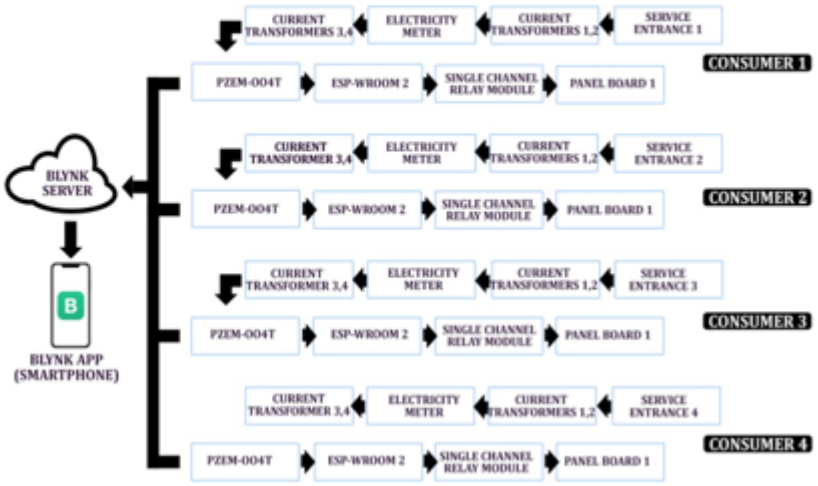
This design focuses on real-time data monitoring in line with the electricity meter and includes an anti-theft feature. A unified network for real-time data exchange is formed by using the PZEM-004T, which facilitates smooth connectivity and communication among the system's components. PZEM-004T measures voltage, current, power consumption, and kilowatt-hours. If abnormal data is collected in the system, it will automatically send a notification to the electricity provider. These data are displayed on the Blynk application, allowing them to monitor the consumers' electricity consumption.

On the other hand, the Blynk server allows the electricity provider to navigate each consumer's data, especially when there are signs of tampering with the consumers' electricity meters. Each system, labeled consumer 1 to 4, represents our electric consumers, whose electricity is monitored by an anti-theft system installed in each of their electricity meters. The consumers have their panel boards labeled PB1, PB2, PB3, and PB4, as they are normally equipped.

In addition to highlighting hardware component integration, this project highlights how various components work in concert to provide a complete anti-theft solution. Redefining security paradigms for a more connected and proactive future, the IoT-based anti-theft system combines sophisticated detection methods with intelligent data management. A notification system will be added for faster data transfer if there are signs of theft.

Figure 3

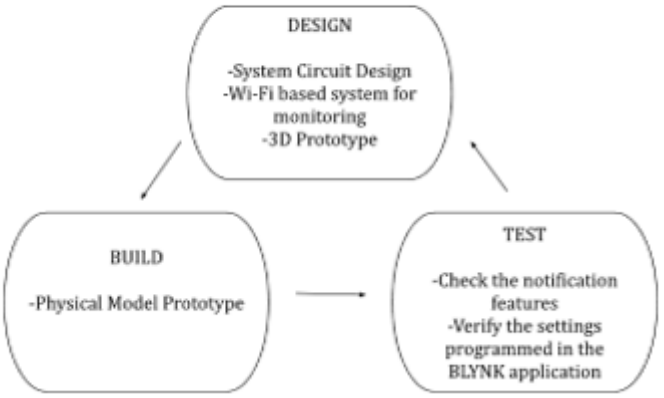
Block diagram interconnection of the proposal project



Research Design

The study's research design is shown in Figure 4. The Design-Build-Test (DBT) Methodology was used in the investigation. Continuous testing is emphasized in this iterative development process. It entails establishing project specifications, generating solution ideas, creating a working prototype, and thoroughly testing it in accordance with those specifications. Design problems that need to be fixed may be discovered during testing. Until a good product is produced, this cycle keeps on. Three circles comprise the research design for this study: the first represents the design phase, the second the build phase, and the third the test phase. An arrow points to the second circle. In the first circle of the study design, the researchers envisioned a Wi-Fi-based system and its circuit. The first circle was where the researchers conceived the Wi-Fi-based system, its circuit design, and the 3D prototype for their study. The second step, "Build," was where the researchers assembled their ideas for the 3D prototype and built a physical prototype for their study. The final step was testing the parameters displayed in the application and assessing the notification features.

Figure 4
Design, build, test methodology



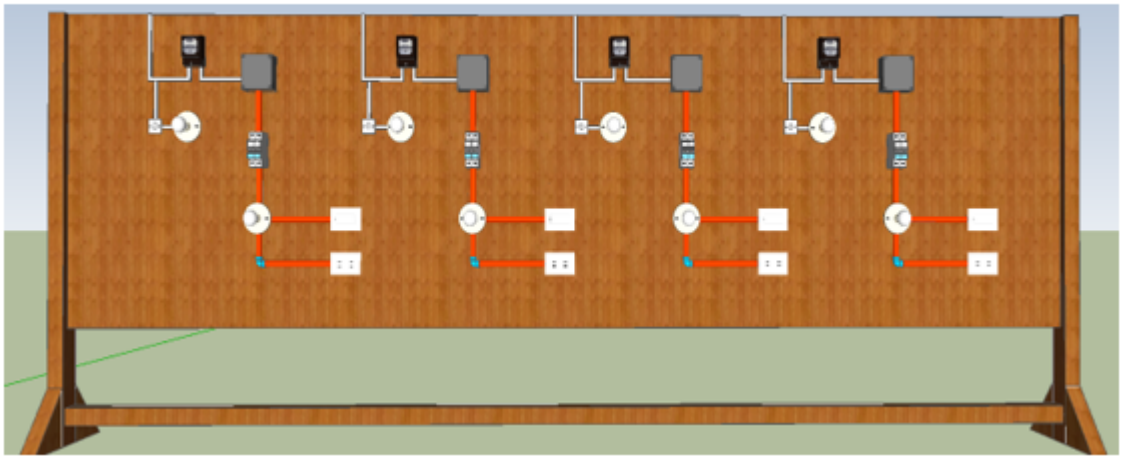
Design Tools

A. Hardware Design

a. SketchUp 3D Model

Figure 5 shows the interconnection layout of the prepaid electricity meter system used. At the core of the system is the microcontroller box, which functions as the central control unit and is directly linked to the main panel board. This main panel board contains the circuit breakers that manage power distribution and operate based on signals from the microcontroller. Positioned beneath the main panel board are four separate circuit breakers, each representing the connection to an individual household's unit's dedicated panel.

Figure 5
Prototype 3D Design



b. Adobe Photoshop

Figure 6 illustrates the power flow diagram of the microcontroller system. The circuits begin with a current transformer connected to the PZEM-004T, with the tapping connections to a standard 230-volt AC power source. The DC power supply converts 230V AC to 12V DC. Then, it passes through the two PZEM-004T that connect to the ESP 32, and the current transformer is connected to the PZEM-004T on the load side.

Figure 6
Power flow diagram of the system

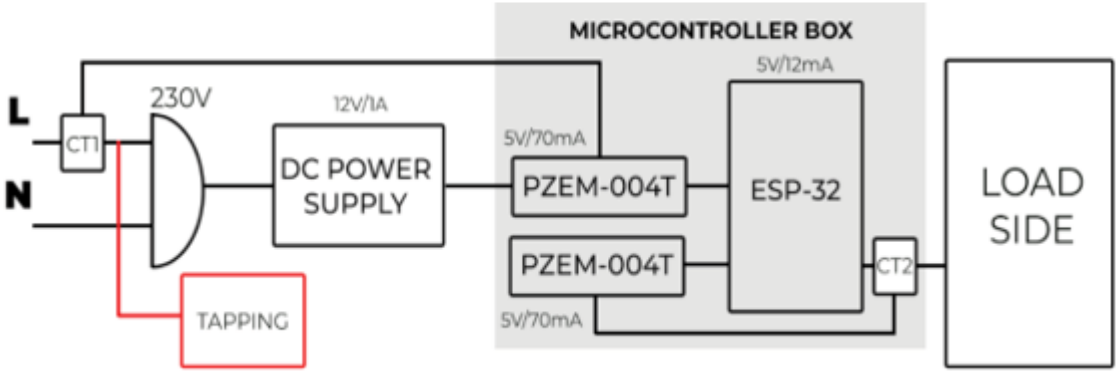
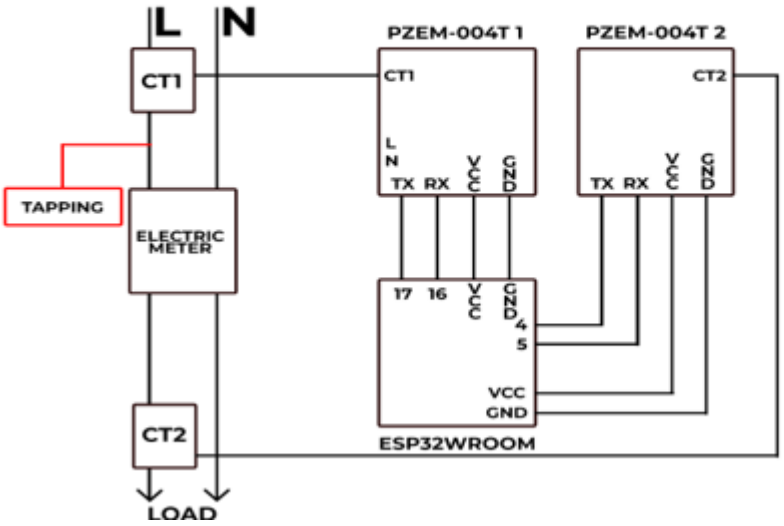


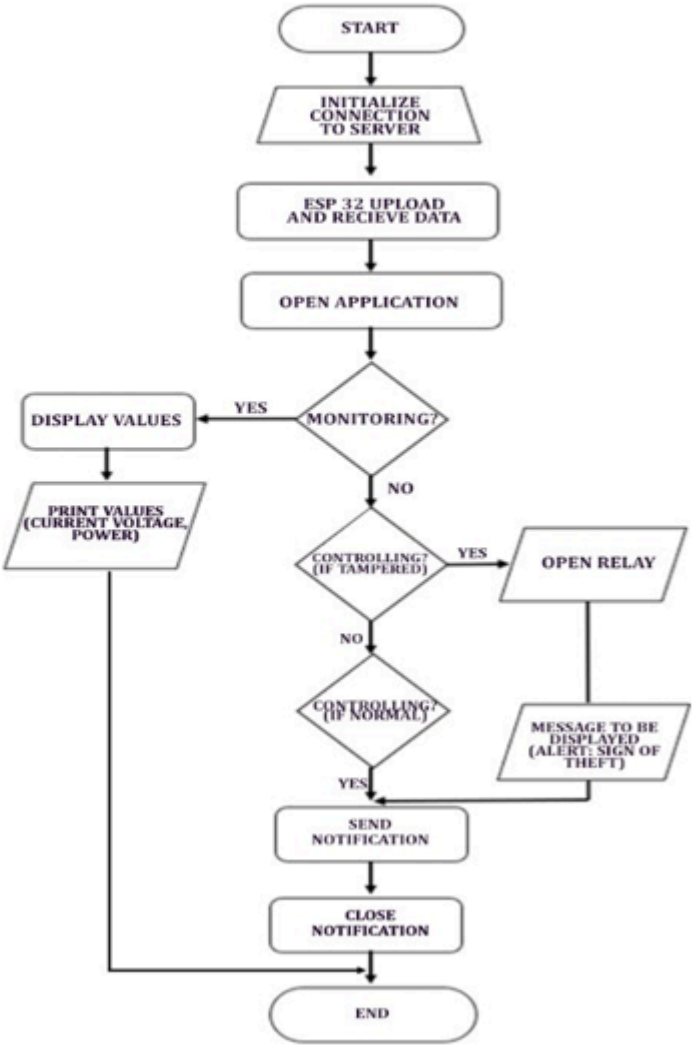
Figure 7 illustrates the schematic diagram of the microcontroller setup for the four households that monitor electricity and detect theft. The PZEM-004T module is connected to the ESP32WROOM microcontroller for communication and control purposes. The TX, RX, VCC, and GND pins are used to measure current, voltage, and kWh. The current transformer is also linked to the PZEM-004T. Note that the current transformer is oriented in a direction that corresponds to the current flow, denoted by an arrow sign. To enable the microcontroller to control power based on PZEM-004T readings, a relay module is also connected to the ESP-WROOM32. Lastly, a 5V power supply powers the ESP-WROOM32.

Figure 7
Schematic Diagram of the Microcontroller



Data Gathering Procedure

Figure 8
Project Flowchart



This outlines the steps involved in gathering data for the project. First, a prototype was built by constructing the electrical components and electronics. This prototype shows the device under study. Next, testing was conducted on the prototype's key characteristics and parameters. To detect the anti-theft feature, the PZEM 004T parameters are compared: current, voltage, power, and kWh. These parameters are compared with a known standard group using statistical methods such as the t-test and group statistics. To assess the prototype's accuracy, percentage-error tests were conducted. This involved calculating the difference between the expected values (measured by instruments like voltmeters and ammeters) and the actual values obtained from the Blynk application. This difference was then divided by the expected value and multiplied by 100% to express the discrepancy as a percentage. A lower percentage error indicates better agreement between the expected and actual performance. The actual performance values of the prototype were also obtained from the Blynk application, which likely monitors the prototype's behavior and displays the relevant data. To ensure accurate comparisons, the prototype was designed to measure voltage and current simultaneously.

Treatment of Data

A fundamental understanding of statistical methods is essential for conducting reliable research, as research involves more than designing experiments and collecting data. Statistical analysis also plays a crucial role in organizing, interpreting, and making sense of the data gathered. The researcher validated the accuracy of the Blynk app readings by comparing them to actual measurements obtained from a voltmeter for voltage and a clamp meter for current. A t-test was used to assess the similarity between the two data sets and determine whether their means differed significantly. At the same time, percent error analysis was used to assess how closely the measured values aligned with the actual values.

To evaluate the system's percentage error, the researchers used the average of both actual measurements from electrical metering tools and expected readings from the Blynk app. Voltage, current, and power were measured over 10 trials, and the mean values for each parameter were computed for both data sources. Equation 1 was then applied to calculate the percentage error using these averages, enabling the researchers to determine the system's overall accuracy.

A dependent t-test, or paired t-test, is a statistical method used in this study to compare the means of two related data sets, where each data point in one set is directly paired with a corresponding point in the other. This test is appropriate when analyzing measurements taken from the same subject or system under different conditions or at different times, allowing the researcher to determine whether a statistically significant difference exists between the paired values.

In conducting a t-test to compare the means of two independent samples, different formulas are applied depending on whether equal population variances are assumed. When equal variances are assumed, the test statistic ttt is computed using Equation (2)

$$t = \frac{\bar{x}_1 - \bar{x}_2}{\sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}}}$$

where the pooled standard deviation sps psp is calculated using Equation (3)

$$s_P = \sqrt{\frac{(n_1-1)^2 s_1^2 + (n_2-1)^2 s_2^2}{n_1+n_2-2}}$$

In these equations, x'1 and x'2 represent the means of the two samples, s1 and s2 are their respective standard deviations, and n1 and n2 are the corresponding sample sizes. The degrees of freedom are determined by df = n1+n2−2. The computed t-value is then compared to the critical value from the t-distribution table. Suppose the computed value exceeds the critical value? In that case, the null hypothesis is rejected, indicating a statistically significant difference between the groups.

In contrast, when the assumption of equal variances is not met, the test statistic is calculated using Equation (4):

$$t = \frac{\bar{x}_1 - \bar{x}_2}{\sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}}}$$

And the degrees of freedom are computed using the Welch–Satterthwaite equation (Equation 5):

$$df = \frac{\left(\frac{s_1^2}{n_1}+\frac{s_2^2}{n_2}\right)^2}{\frac{\left(\frac{s_1^2}{n_1}\right)^2}{n_1-1}+\frac{\left(\frac{s_2^2}{n_2}\right)^2}{n_2-1}}$$

This approach, known as Welch's t-test, does not require the assumption of equal variances and adjusts both the test statistic and the degrees of freedom accordingly. As with the equal variance case, the null hypothesis is rejected if the calculated t-value exceeds the critical value from the t-distribution.

DATA AND RESULTS

Hardware Development

A. Constructing the frame

In the frame construction, the plywood was accurately cut using a saw to ensure conformity with the dimensions outlined in the 3D model. A wooden framework was constructed to support the plyboard in an upright orientation, with two wooden stands secured to the plyboard employing wood screws. To further enhance stability, a wooden base was positioned between the two frames that support the plyboard. Finally, a coat of paint was applied to elevate the aesthetic quality.

Figure 9
Installed components of microcontroller box

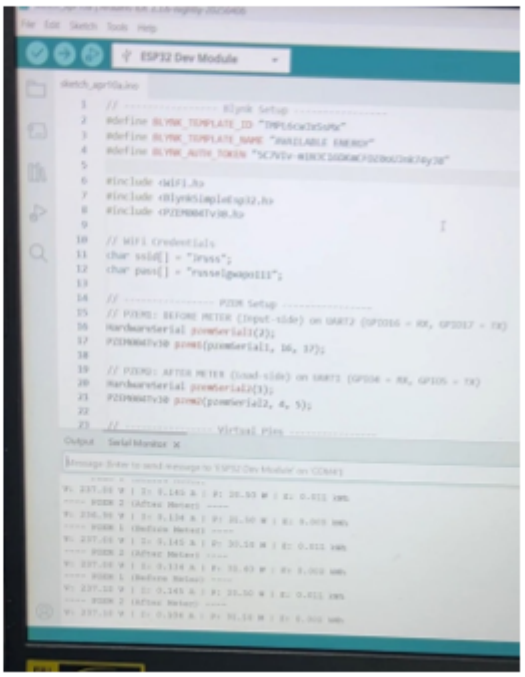
Figure 10
Complete prototype

Software Development

A. Coding with Arduino IDE Software

The Arduino IDE was used for programming and integrating with the components, which include the ESP-WROOM32, PZEM-004T sensor, and current transformers. The first step was constructing the code and compiling it. After the code had been successfully compiled without errors, it was uploaded to the microcontroller.

Figure 11
Serial Print of Data Values



As shown in Tables 1 and 2 below, these values were used in order to perform percentage error calculation to determine the difference between the actual values from PZEM 1

and PZEM 2, respectively.

Table 1
PZEM 1 Percent Error Test

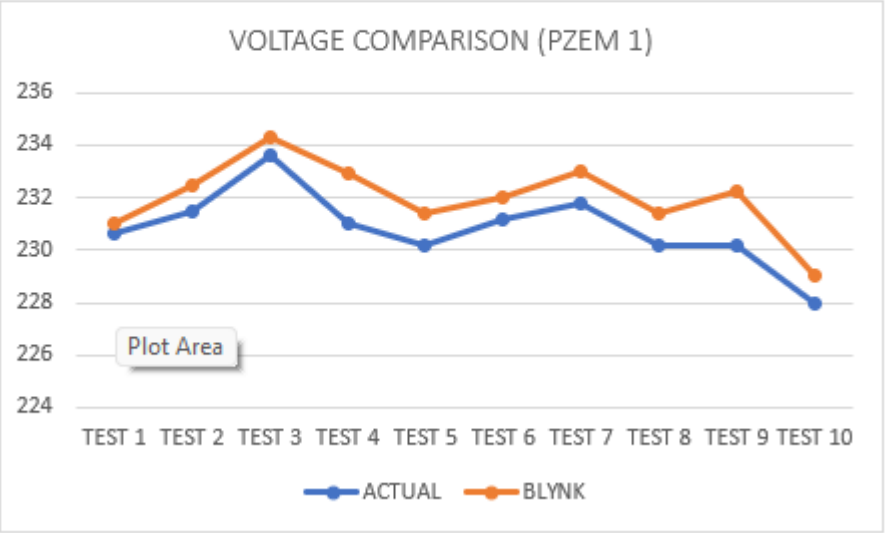
	Mean			
	n	**Actual**	**Expected**	**%Error**
Voltage(V)	10	231.1889	232.4333	0.5353984
Current(A)	10	1.682	1.702	1.1750881
Power(W)	10	388.3834	395.074	1.6935055

Table 2
PZEM 2 Percent Error Test

	Mean			
	n	**Actual**	**Expected**	**%Error**
Voltage(V)	10	230.47	231.69	0.52657
Current(A)	10	1.642	1.662	1.20337
Power(W)	10	378.4918	385.1256	1.7225

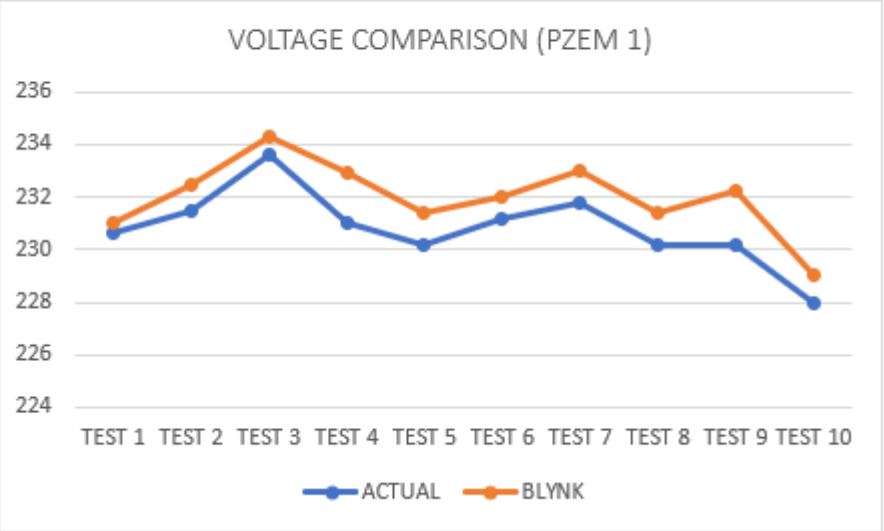
Blynk Application and Voltmeter Comparison

Figure 12
Voltage comparison between Blynk and voltmeter in PZEM 1



A voltmeter was connected in parallel with the device to measure its voltage. This configuration is crucial because components connected in parallel experience the same potential difference. Connecting the voltmeter in parallel ensured that it measures the same voltage drop as the device in the circuit.

Figure 13
Voltage Comparison between Blynk and Voltmeter in PZEM 2



Tables 3 and 4 present the descriptive statistics of voltage measurements obtained from two devices—Blynk and a Voltmeter—across two different PZEMs. For the Blynk device, both sets of measurements (n = 10) yielded mean voltages of 232.09 V and 231.69 V, with standard deviations of 1.4547 V and 1.3579 V, and standard errors of the mean at 0.4255 V and 0.01765 V, respectively. The Voltmeter readings, also based on ten samples, showed mean voltages of 321.37 V and 230.47 V, accompanied by standard deviations of 1.4547 V and 1.3579 V. Standard errors of 0.46001 V and 0.4394 V. These results suggest that Blynk provided voltage readings with marginally higher average values and slightly lower variability compared to those of the Voltmeter.

Table 3
T-test Group Statistics Comparing Blynk and Voltmeter in PZEM 1

Voltage(V)	n	Mean	Std. Deviation	Std Error Mean
Voltmeter	10	230.8700	1.3579	0.4294
Blynk	10	232.0900	1.3065	0.4131

Table 4
T-test Group Statistics Comparing Blynk and Voltmeter in PZEM 2

Voltage(V)	n	Mean	Std. Deviation	Std Error Mean
Voltmeter	10	230.47	1.3579	0.4294
Blynk	10	231.69	0.0558	0.01765

Blynk Application and Ammeter Comparison

Figure 14
Current comparison between Blynk and Ammeter in PZEM 1

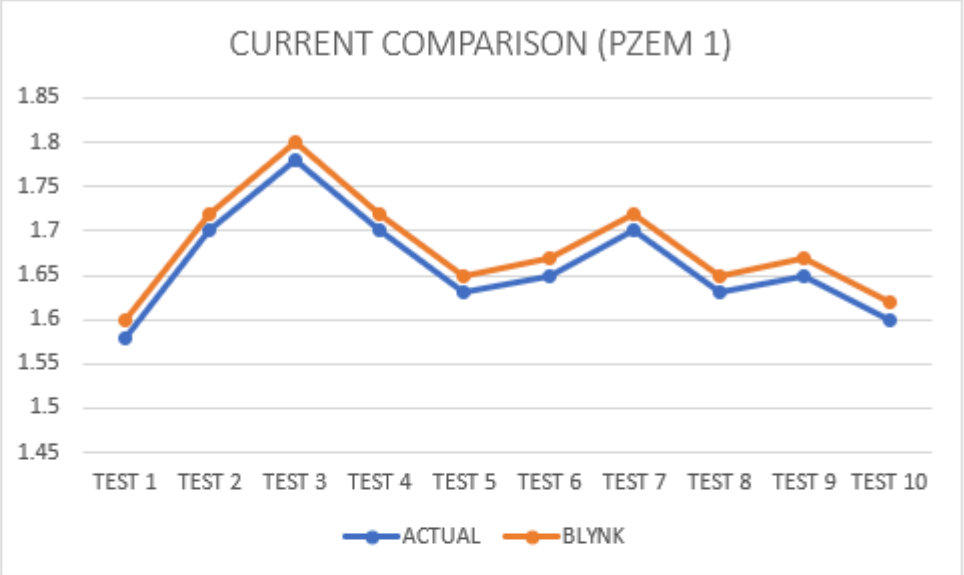


Figure 15
Current comparison between Blynk and Ammeter in PZEM 2

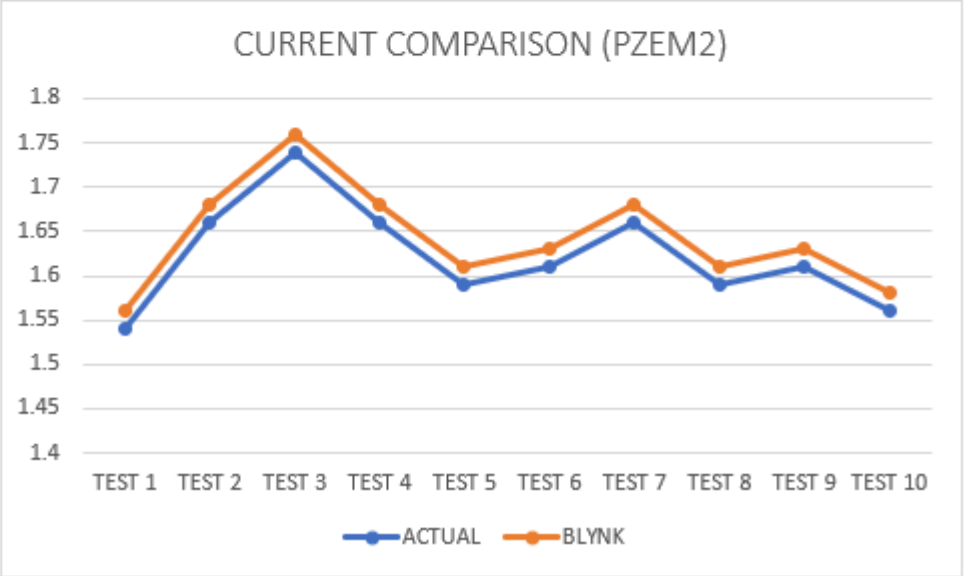


Table 5
T-test group Statistics Comparing Blynk and Ammeter in PZEM 1

Current(A)	n	Mean	Std. Deviation	Std Error Mean
Ammeter	10	1.6820	0.05585	0.0177
Blynk	10	1.7020	0.05583	0.01765

Table 6
T-test group Statistics Comparing Blynk and Ammeter in PZEM 2

Current(A)	n	Mean	Std. Deviation	Std Error Mean
Ammeter	10	1.642	0.0558	0.0177
Blynk	10	1.662	0.0558	0.01765

Tables 5 and 6 present descriptive statistics for current measurements obtained from two different devices, Blynk and a voltmeter, across two PZEM setups. For Blynk, with a sample size of 10, the recorded mean currents are 1.7020 A and 1.662 A, accompanied by standard deviations of 0.05583 A and 0.0558 A, and standard errors of 0.01765 A for both sets. Similarly, the voltmeter (acting as an ammeter) yields mean currents of 1.6820 A and 1.642 A, with standard deviations of 0.05585 A and 0.0558 A, and standard errors of 0.0177 A. These results demonstrate that both devices exhibit nearly identical mean values and variability in current measurements, indicating a high level of consistency between the Blynk and voltmeter readings.

Figure 16
Current comparison between Blynk and Ammeter

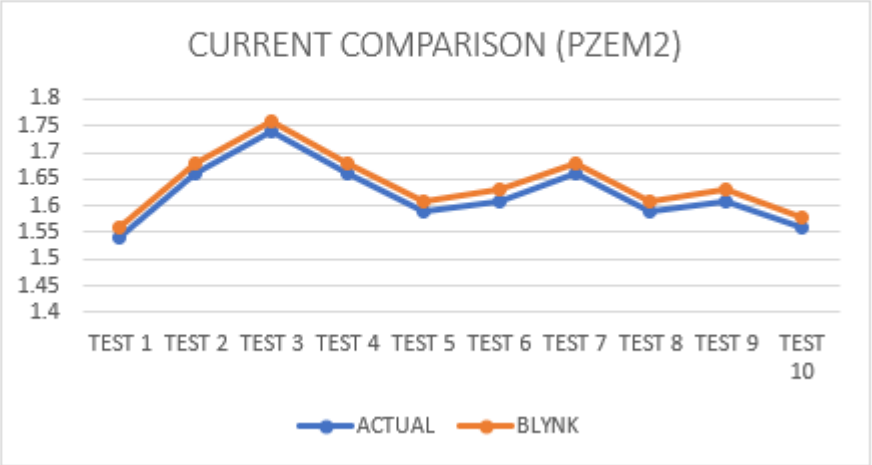


Figure 17
Power comparison between Blynk and Calculate actual value in PZEM 1

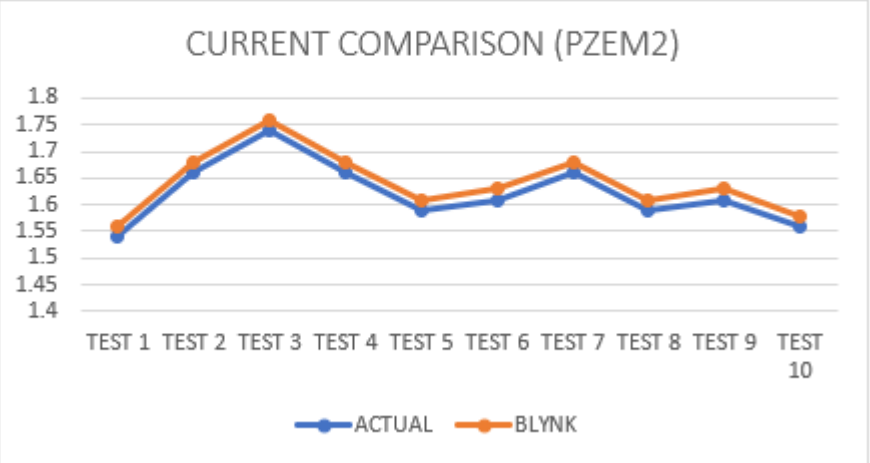


Figure 18
Power Comparison between Blynk and Calculated Actual Value in PZEM 1

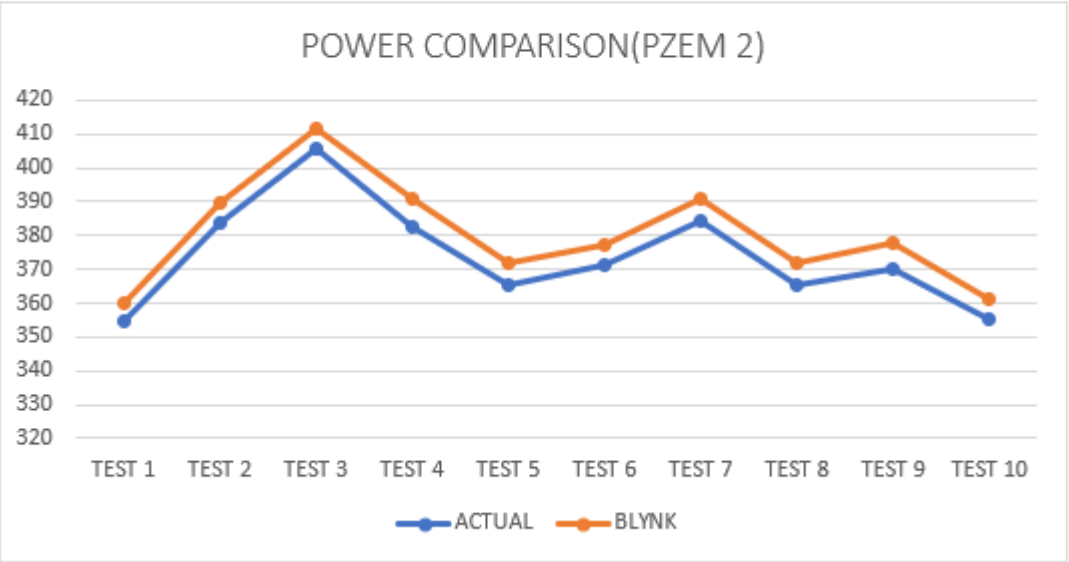


Table 7
PZEM 1 t-Test Group Statistics

Power(W)	n	Mean	Std. Deviation	Std Error Mean
Actual	10	388.3834	14.8128	4.6842
Blynk	10	395.0740	14.7879	4.6763

Table 8
PZEM 2 t-test group statistics

Power(W)	n	Mean	Std. Deviation	Std Error Mean
Actual	10	378.492	14.7447	4.6627
Blynk	10	385.126	14.7221	4.6555

Tables 7 and 8 summarize power measurements obtained using the Blynk application and a calculated method, with 10 trials conducted for each approach across both PZEM units. The average power recorded via Blynk was 395.07 W and 385.126 W, which is slightly higher than the corresponding calculated averages of 388.3834 W and 378.492 W. Despite this marginal difference, both methods exhibited comparable standard deviations of approximately 15 W, indicating that the power values are consistently distributed around their respective means. Furthermore, the standard error for both methods remained close to 4.6 W, suggesting low variability and reinforcing the precision and reliability of the results. Collectively, the data in Tables 11 and 12 demonstrate strong agreement between Blynk-measured and calculated power values, validating the accuracy and consistency of both measurement approaches in this experiment.

Comparison of Data with and without Electricity Theft

Table 9

Differences between the Measured Parameters

	n	Without Tapping	With Tapping	Difference
VOLTAGE(V)	10	230.57	231.31	-0.74
CURRENT(A)	10	0.8287	0.8887	-0.06
POWER(W)	10	191.0401	205.20215	-14.16205

Table 9 presents a comparative analysis of voltage, current, and power measurements under two conditions: without tapping (normal operation) and with tapping (simulated electricity theft). Each condition includes ten recorded trials. The data reveals a subtle increase in voltage and current during the tapping condition, with voltage rising from 230.57 V to 231.31 V and current from 0.8287 A to 0.8887 A. In contrast, these differences are 0.74 V and 0.06 A. It may appear minor, but its impact on the resulting power measurements is significant. Power consumption increased from 191.0401 W under normal conditions to 205.20215 W with tapping, resulting in a notable discrepancy of -14.16205 W. This increase in recorded power, despite only slight variations in voltage and current, suggests unauthorized energy usage indicative of electricity theft. The data underscore the sensitivity of power monitoring systems to even small-scale tampering or unauthorized tapping, reinforcing the importance of precision in current and voltage measurements to ensure the integrity and security of electrical systems. Ultimately, the results in Table 8 validate the system's capability to identify discrepancies caused by illicit consumption, highlighting its potential role in theft detection and energy accountability.

CONCLUSION AND RECOMMENDATIONS

The researchers conducted thorough testing of the electricity monitoring system with an anti-theft feature to confirm its reliability and functionality. The following verifications indicate the achievement of the study's objective: the researchers successfully created a design for their prototype using SketchUp and Adobe Photoshop to connect the system's main components. The researchers managed to build a Wi-Fi/ smartphone-based real-time electricity monitoring system with an anti-theft system that allows the electricity provider to be notified once a house's electricity meter has been tampered with. The researchers verified the proper functioning of their electricity monitoring system, including its anti-theft feature, by testing each component both separately and as an integrated unit. They employed measuring instruments to collect data, ensuring the system's effectiveness, precision, and dependability.

Recommendations

The preceding suggestions are intended to support upcoming investigations and research projects aimed at enhancing the current methodology.

- Employ digital meters for accurate data comparison: Future studies should utilize digital meters to accurately compare the data recorded by the Blynk application with the readings from the energy meter.
- Utilize polypropylene enclosures for microcontrollers to reduce Wi-Fi signal interference: Future research should consider using polypropylene enclosures to minimize interference with Wi-Fi signals in microcontroller applications.

- Investigate CT sensor detection at low load levels: Future studies should focus on the ability of CT sensors to detect devices even under low load conditions effectively.
- Implement AVR transformers to maintain stable voltage output: Future research should emphasize the use of AVR transformers to ensure reliable and consistent voltage levels in electrical systems.
- Explore the implementation of GSM modules for offline notifications in IoT Devices: Future research should investigate the use of GSM modules to enable IoT devices to send alerts even when they are not connected to the internet. Put an enclosure around the current transformer before the Electric Meter.

REFERENCES

Andaya et al. (2018) *Detection system of electricity theft at service conductors of elevated metering centers*. https://ejournals.ph/article.php?id=12319

Madhu G M et al.(2020), *Internet of things enabled power theft detection and smart metermonitoringsystem*.https://www.researchgate.net/publication/344056693_Internet_of_Things_Enabled_Power_Theft_Detection_and_Smart_Meter_Monitoring_System

Manisha Sharma et al. (2016), *Internet of things-based smart electricity meters.* https://www.researchgate.net/publication/290787813_Internet_of_Things_based_Smart_Electricity_Meters

Shady Y. Mtair et al. (2024*). A smart energy monitoring system using an ESP32 microcontroller*.https://www.researchgate.net/publication/381813421_A_Smart_Energy_Monitorin g_System_using_ESP32_Microcontroller

Siano, P. (2016). *A review of smart cities based on the internet of things concept*. https://scholar.google.com/citations?view_op=view_citation&hl=en&user=bSvAqDUAAAAJ&citation_for_view=bSvAqDUAAAAJ:tH6gc1N1XXoC