FUDMA Journal of Engineering and Technology
ISSN: 3092-9385
https://sites.google.com/fudutsinma.edu.ng/fjet
Volume 1, Issue 2, 2025, 57-67

A Microcontroller-Based Intelligent Electricity Theft Detection and Prevention System

Damilare L. ADEKEYE[1*], Uche M. IROKA[2]

[1,2]Department of Electrical & Electronics Engineering, Federal University of Technology, Minna, Nigeria

[1*]adekeyedamilarelekan@gmail.com, [2]mosesiroka@gmail.com

Abstract

Electricity theft is a major non-technical loss affecting the power sector, wherein consumers bypass energy meters to consume more electricity than paid for. This practice poses a significant financial threat to utility providers, resulting in revenue losses and hindering the development of the power industry. Various research efforts have explored techniques to curb electricity fraud, including communication systems, the Internet of Things (IoT), and machine learning. However, challenges persist due to inadequate real-time monitoring and ineffective tracking of consumption patterns. To address this issue, this paper proposes a microcontroller-based electricity theft detection system utilizing the Arduino ATmega328P for intelligent monitoring. The system incorporates a GSM module, current and voltage sensors, a relay, and a keypad interface. The system was tested under two conditions, normal operation and operation with bypass load, across 10 different load scenarios. It achieved 100% classification accuracy, successfully detecting all five cases of electricity theft while maintaining uninterrupted service for the remaining five authorized loads. Experimental results confirm the system's ability to detect unauthorized load connections, automatically trip the relay to cut off power, and send a theft alert via SMS. Reactivation of the system requires the input of an authenticated password through the keypad module. The proposed system demonstrates high effectiveness in real-time theft detection, offering a cost-effective and reliable solution for improving power distribution security and minimizing non-technical losses.

Keywords: *Electricity theft, Arduino, relay, energy meter, current sensor.*

1.0 Introduction

Electrical energy is an integral resource for the economic development of every nation. It is essential for enhanced industrial production activities, thereby improving the overall quality of life in society. Consequently, the degree of electric energy consumption per capita can serve as a measure for estimating the standard of living in a country.

The processes of electrical energy generation, transmission, and distribution involve various operational losses. While generation losses can be technically defined, transmission and distribution losses are often difficult to quantify using only sending-end information, highlighting the influence of non-technical parameters in these systems. Technical losses occur naturally due to power dissipation in transmission lines, transformers, and other power system components [1].

There are two primary types of electric power losses in the power system: technical and non-technical. Technical losses result from faults in cables, transformers, overhead lines, and other substation equipment within the distribution network [2]. Non-technical losses arise mainly from illegal activities, such as cable theft, non-payment of tariffs, usage of fraudulent prepaid vouchers, meter tampering, and unauthorised electricity connections [3][4].

Energy theft poses a significant threat to power system stability and revenue. It manifests in various forms, including meter tampering and meter inversion, where users manipulate readings to underreport actual consumption. Several countermeasures are being deployed, such as smart meters, advanced software solutions, and regulatory enforcement [5]. Additionally, methods incorporating communication meters, smart applications, and detection algorithms like Support Vector Machines (SVM) and Fuzzy Inference Systems (FIS) have been applied to detect theft activities like direct hooking and short-circuiting [6].

A comprehensive approach to theft prevention involves monitoring both at the consumer end and at centralized control units, typically facilitated by GSM-based communication and display modules. Smart metering and advanced theft detection systems have garnered increased attention for minimising manual interventions and bribery [7].

Given the increasing rate of theft and meter tampering, this study proposes a microcontroller-based electricity theft detection system capable of real-time monitoring and alert generation. The system is designed to detect illegal activities at the consumer site and notify utility providers with precise time and location information. The objectives include designing, implementing, and testing the system's circuit functionality. This approach offers an innovative and scalable solution to address the growing challenge of electricity theft.

Received: 02/07/2025; Revised: 07/07/2025; Accepted: 08/07/2025; Published: 08-08-2025

Several existing methods have incorporated microcontrollers, GSM modules, IoT, and smart metering technologies. Advanced metering infrastructure (AMI) plays a crucial role in smart grids, offering capabilities such as demand response and real-time load management.

In [8], a pattern-based detection system was developed to monitor abnormalities using transformer meters and clustering techniques. Although privacy-conscious and efficient, it depends heavily on predefined user behaviour patterns. An IoT-based solution presented in [9] utilised an Arduino MKR1000 and PIR sensors to detect unauthorized access and transmit data to the cloud. While effective, it relies on consistent internet availability, which may limit deployment in rural areas.

Similarly, a high-voltage-based anti-theft system was designed in [10] to interrupt illegal connections. However, its brief power suspensions affected legitimate users and posed risks to appliances. In [11], a supervised learning model combining ADASYN, VGG-16, and a Firefly Algorithm-enhanced XGBoost classifier achieved high accuracy, but required heavy computation, limiting real-time usability.

A system based on Extreme Gradient Boosting (XGBoost) was developed in [12], achieving better accuracy than SVM and decision trees. Nonetheless, its reliance on labelled attack data restricts adaptability to new tactics. A deep learning approach in [13] used time-frequency features and Bayesian tuning, achieving a 97% AUC, though at high computational cost.

In [14], a focal loss-based 1D DenseNet detected theft using historical data, achieving 98.51% accuracy. However, its complexity hinders deployment in low-resource settings. A 15-year review in [15] identified ML and statistical models, such as ARIMA and Bayesian networks, as prevalent in fault detection. Challenges included data imbalance and real-time adaptability.

A GSM-based monitoring system for transformers was presented in [16], focusing on fault diagnosis but lacking theft detection capabilities. A smart metering system in [2] using an Arduino ATMega328P and GSM modules detected abnormalities and sent SMS alerts, but its reliance on cloud storage posed limitations in underdeveloped areas.

Despite progress, many existing methods suffer from computational demands, high false positives, and internet dependence. The proposed system addresses these issues by combining real-time current monitoring with GSM-based notifications. Unlike data-intensive machine learning models, this system leverages microcontroller simplicity and reliable GSM communication to deliver fast and accurate alerts.

The approach balances accuracy and feasibility, avoiding the need for high-cost infrastructure or risky high-voltage techniques. The use of onboard ADC converters in the Arduino enhances automation and precision, improving upon limitations in previous designs.

Section Two presents the detailed design and implementation process of the proposed system. Section Three covers the testing phase, evaluating system performance under specific metrics. Section Four concludes the study and outlines recommendations for future enhancements

2.0 Methodology

This section details the design methodology and the implementation of the intelligent electricity theft detection system. The analysis began with brief explanations of the system components, followed by the system hardware development. The development of the software operation algorithm with the integration stage is provided for proper insight into the system development and operation theory.

2.1 Materials/Components

The major components utilised in the development of the proposed system are explained as follows;

i. Arduino UNO

The Arduino UNO is an open-source microcontroller board that is inexpensive, versatile, and simple to use. It can be used in various types of electrical projects. This board can be interfaced with other Arduino boards, Arduino shields, and Raspberry Pi boards and can operate relays, LEDs, servos, and motors as an output.

ii. Liquid Crystal Display

The light-modulating capabilities of liquid crystals in conjunction with polarisers are utilised by liquid-crystal displays (LCDs), which are flat-panel displays or other electronically manipulated optical devices. Instead of emitting light directly, it creates colour or monochrome pictures via a backlight or reflector.

iii. SIM800L GSM Module

The SIM800L module is a miniature GSM Module that supports quad-band GSM/GPRS network, meaning it works pretty much anywhere in the world. The module supports baud rates from 1200bps to 115200bps with Auto-Baud detection. The module has a Helical Antenna, which is soldered directly to the NET pin on the PCB. Also, it has a UFL connector facility if you want to keep the antenna away from the board. There is an LED on the top right side of the module which indicates the status of the cellular network.

iv. Single Pole Single Throw (SPST) Switch

A Single-Pole, Single Throw (SPST) switch is a switch which features a single input terminal and one output terminal. A one-pole one-throw switch serves in circuits as an on-off switch. When the switch is closed, the circuit is on. When the switch is open, the circuit is off.

v. Relay

Relays are electrical appliances that use a low voltage to control a higher one. A relay could come as either electromechanical or in solid-state form, performing similar functions, only differing in efficiency. Higher loads are controlled by static relays, whereas lower loads are controlled by electromechanical relays. The project's relay is an electromechanical relay with a rating of 10A, and it performs the circuit function of tripping off the loads when it receives the prompt from the microcontroller.

vi. Buck converter

A buck converter or step-down voltage regulator is a type of DC-DC converter (switching converter). It is a converter that reduces the input DC voltage to a specified DC voltage. More power efficiency is provided by it as a DC-DC converter than a linear regulator. Due to its high efficiency, the buck converter is useful for tasks such as converting a computer's main supply voltage down to the lower voltage needed by USB, CPU, and so on.

vii. Current Sensor

When an electrical current flow across a wire, a current sensor detects it and produces a signal that is proportionate to the current. The signal that is produced may be a digital output or an analogue voltage, or a current. Following that, the created signal can be used to control a device, save data for further analysis in a data acquisition system, or show the measured current in an ammeter.

viii. Voltage Sensor

A voltage sensor is a device that measures voltage. Voltage sensors can measure the voltage in various ways, from measuring high voltages to detecting low current levels. These tools are necessary for many applications, including industrial and power systems control.

ix. Real-Time Clock

A real-time clock, or RTC, is a digital clock with the primary function of keeping accurate track of time even when a power supply is turned off or a device is placed in low-power mode. RTCs are comprised of a controller, oscillator, and an embedded quartz crystal resonate.

2.2 Method

Figure 1 illustrates the techniques employed in the development of the proposed theft detection system. It began with the design of the hardware part and the development of the software system that coordinates the operation sequentially. Finally, the integration of the software package into the microcontroller and the packaging of the system prototype.

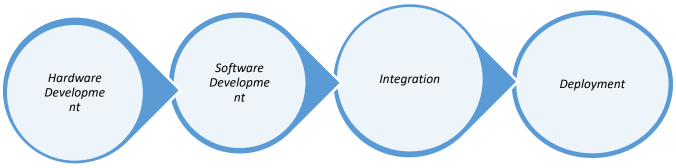


Figure 1: System Development Process

2.2.1 System Hardware Development

Development of a hardware system requires careful component selection and circuit design for seamless communication and data transfer between the devices. This is essential to ensure adequate system functionality. In this section, the component specifications and circuit design are discussed accordingly before the development and implementation stages. The hardware system comprises three significant modules: power module, sensing module and communication module.

i. Power Module

The power supply circuit makes up the majority of the Power Module. This circuit uses the Zener power regulation technique to regulate two voltage levels of 5V and 12V DC, respectively. It includes a current-limiting capacitor, a bridge rectifier, filtering capacitors, a Zener diode, a buffer transistor, and a three-terminal adjustable voltage regulator. The LCD and Microcontroller are powered by 5V, and the Relay by 12V. For the rectification circuit, the 2W005G bridge rectifier, which features a diffused junction, a low forward voltage drop of 1V, a high current capacity of 50A, and an average rectified output current of 2A, makes up the rectification circuit. To determine the output rectifier voltage (V_{ip}),

$$V_{ip} = \sqrt{2} \times V_{rms} \times k - (2 \times V_D) \qquad (1)$$

where: $Vrms$ =220V, V_D =Diode voltage (0.7V) and k= scaling factor (0.05)

Moreover, the capacitors C4 and C5 in the power circuit enable filtering and reduce the amount of ripples present in the circuit. The operating voltage is given as in equation (2), where the peak voltage and root mean square voltage relation is given as shown in equation (3),

$$\mathrm{V_{wv}} \geq 2\,\mathrm{V_p} \qquad (2)$$

where V_{wv} = working voltage, V_P= peak voltage.

$$\mathrm{V_p} = \sqrt{2} \times \mathrm{V_{rms}} \qquad (3)$$

Equation 4 is used to determine the ripple voltage, considering a 12 V DC voltage chosen in this study,

$$\mathrm{V_{yrms}} = \mathrm{y} \times \mathrm{V_{L(DC)}} \qquad (4)$$

where $\mathrm{V_{yrms}}$ = ripple voltage, y = ripple factor (0.482), and $\mathrm{V_{L(DC)}}$ =dc load voltage (12V).

The capacitance (C) value can be obtained from the current formula of the capacitor given as in equation 5. It can also be re-expressed in terms of voltage, frequency, and the ripple factor, as illustrated in Equation 6,

$$i_c = \frac{dq}{dt} = C\frac{dv}{dt}, \qquad (5)$$

where q = charge in coulomb, q = CV.

$$\mathrm{C} = \frac{\mathrm{i_{dc}}}{4\sqrt{3\,\mathrm{fyV_{ip}}}} \qquad (6)$$

where, f = 50Hz, $\mathrm{V_{ip}}$ = output rectifier voltage, $\mathrm{i_{dc}}$ = DC load current.

It can be deduced that the least capacitor value needed is 423μ∫, to get a high value of voltage; we require a large value of capacitance in the circuit. Thus, a capacitor with a value of 1000μ∫ was chosen. Which is more than twice the value needed. This is used to provide safety in the circuit. Therefore, C4 and C5 are rated 1000μ∫. The power module circuit diagram is shown in Figure 2.

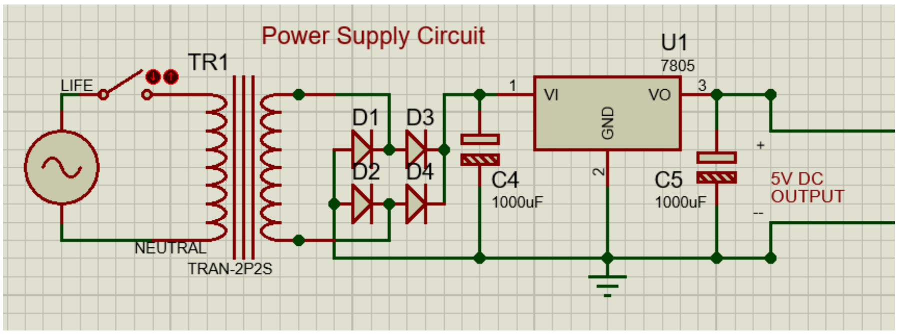


Figure 2: Power circuit diagram

ii. Sensing Module

In the realm of electronic systems and energy management, current and voltage sensing modules stand as crucial components, providing valuable insights into the flow and potential of electrical energy. These sensing modules play a pivotal role in monitoring, controlling, and optimising power-related processes across various applications, from industrial machinery to renewable energy systems and smart grid implementations.

Current sensors, designed to measure the flow of electric current through a conductor, offer a real-time understanding of power consumption and enable precise current monitoring. Simultaneously, voltage sensors

Received: 02/07/2025; Revised: 07/07/2025; Accepted: 08/07/2025; Published: 08-08-2025

measure the electrical potential difference in a circuit, providing essential information about the voltage levels and aiding in voltage regulation.

iii. Controller Module

This is the brain of the entire circuit. This is where information is received, processed, and sent to other units. The major component of this unit is an Arduino Uno (ATMEGA328p).

iv. Communication module

The communication module's two main parts are the microcontroller and the GSM module. The TX pin of the GSM module is linked to the RX pin of the controller, and the RX pin of the controller is connected to the TX pin of the GSM module. The GSM module's power is linked to the VCC pin source, and the GND is grounded. The GSM module notifies the user via SMS when there is a bypass in the electrical distribution by sending a signal to the GSM module.

The overall system architecture is represented in Figure 3. However, the resulting circuit diagram drawn with Proteus software is as shown in Figure 4.

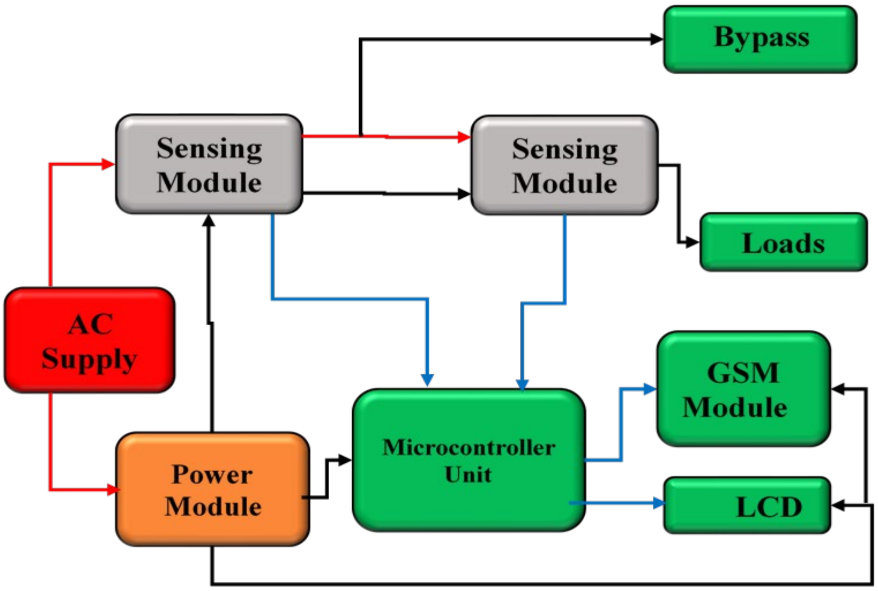


Figure 3: Block Diagram of the system set-up

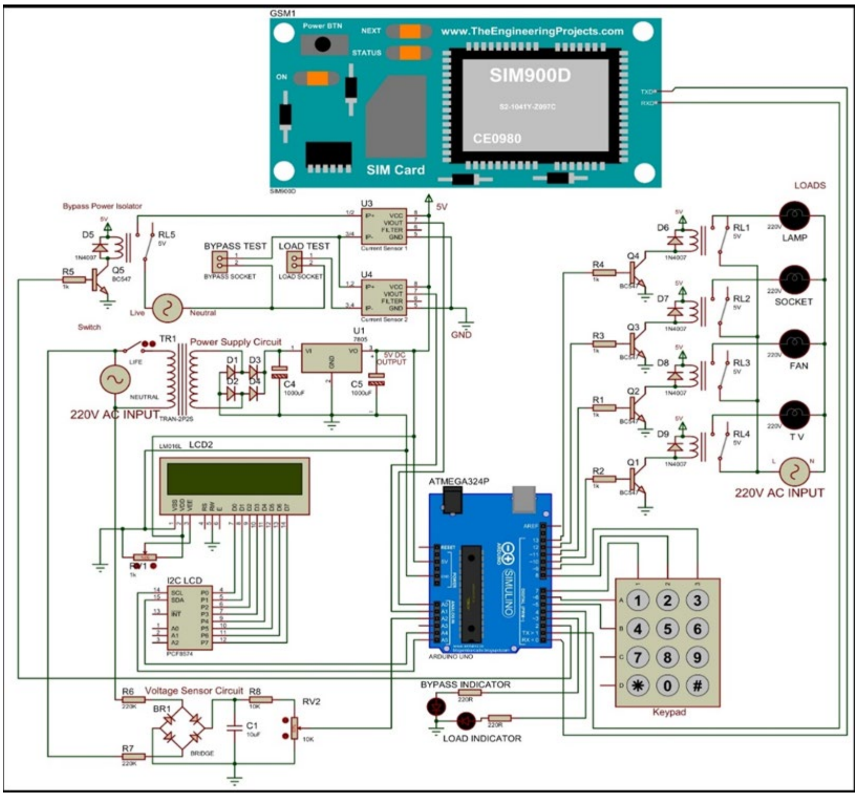


Figure 4: Complete circuit diagram

Received: 02/07/2025; Revised: 07/07/2025; Accepted: 08/07/2025; Published: 08-08-2025

2.2.2 Software Development

The software program is embedded into the hardware setup through the microcontroller chips to coordinate the system's operation flow. This microcontroller is responsible for executing the instructions stored in the program memory. The ATmega328P relies on an external crystal oscillator (usually 16 MHz) to provide the clock pulses for its operations. The clock frequency determines the rate at which the microcontroller processes instructions. The Arduino Uno is programmed using the Arduino Integrated Development Environment (IDE). The code is written in a simplified version of C/C++ and uploaded to the ATmega328P.

The ATmega328P features a set of digital and analogue pins that serve as input or output. These pins allow communication with external devices and sensors, enabling the Arduino Uno to interact with the surrounding environment. The Arduino Uno's digital pins can be configured as either inputs or outputs, dealing with binary signals (0 or 1). Analogue pins, although primarily digital, can also read analogue signals, enabling the board to process continuous voltage levels. The ATmega328P incorporates various peripheral modules, including timers/counters, serial communication (UART), interrupts, and analogue-to-digital converters (ADC). These features enhance the microcontroller's capabilities for handling diverse tasks.

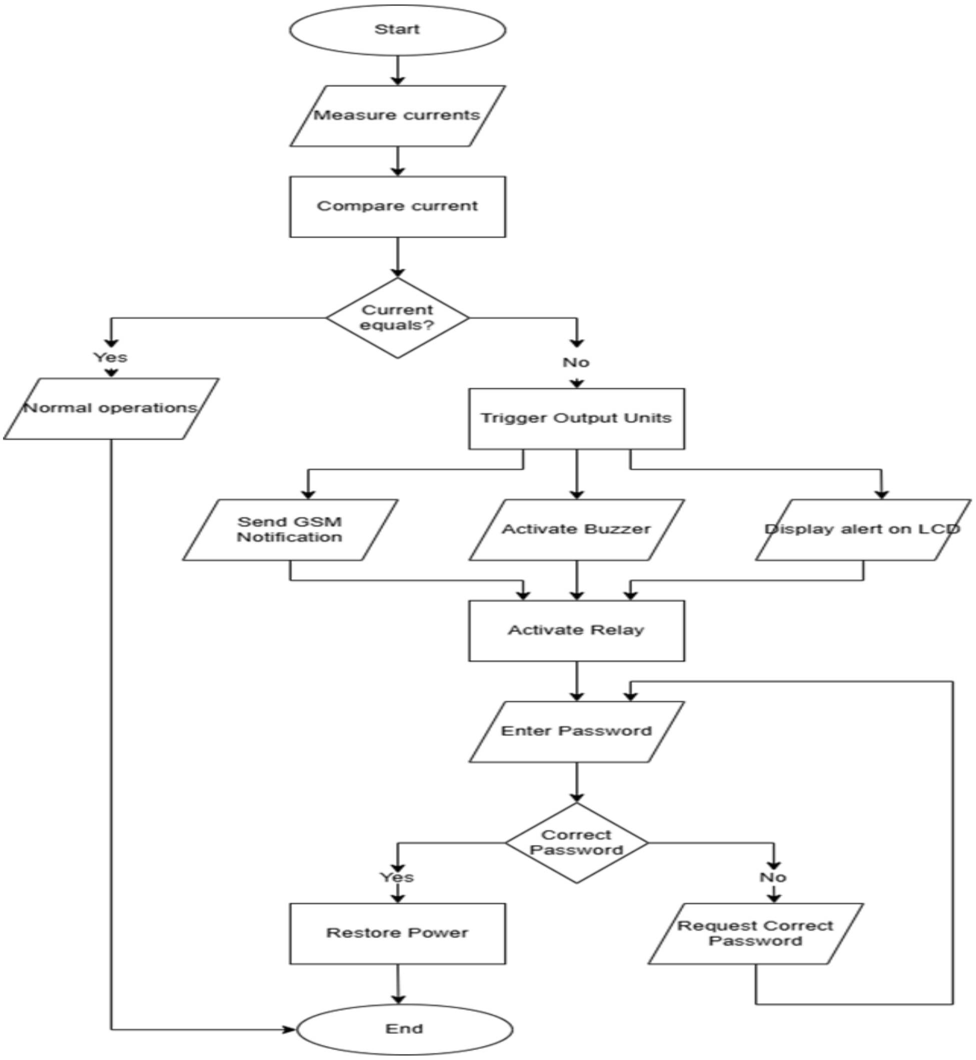


Figure 5: System Operation Flow Chart

Figure 5 illustrates the operational description of the proposed system, which is coordinated by the instructions uploaded on the ATmega328P. The system operates on two current sensors, one on the pole line and the second one installed on the energy meter. The current sensors measure the current across the line. These values are converted to DC inside the sensors and provided to the ADC (Analogue to Digital Conversion) input of the Arduino. The program was written for the Arduino to compare these two values in Arduino language.

If there is any difference between the two values, it will detect the occurrence of power theft between the two current sensors. Then the Arduino will detect and display the status on the LCD module. At the time of theft occurrence on the load side, the power line of the victim customer will be interrupted. The buzzer is triggered, followed by a message sent to the power authority from the GSM module. Afterwards, the system goes out, and

Received: 02/07/2025; Revised: 07/07/2025; Accepted: 08/07/2025; Published: 08-08-2025

a password is requested to initialise it. If the password is authenticated, the system resumes the loop of comparing the current; else, the system ends.

2.2.3 System Integration and Implementation

The hardware components are integrated with the algorithm designed at the software development stage. All components are amalgamated to ensure seamless interaction and uninterrupted operation of the system. The focus at this stage is on assembling the hardware system, interfacing the components, and software embedding.

The process involves combining hardware and software devices to build a functional prototype. It generally includes component interfacing, power module synchronism, and communication integration. The communication synchronisation part provides the intelligent functionality of the system. It includes the GSM module that notifies the authority of the detected fraud event. The Arduino was programmed to trigger a theft notification to enable quick action by the utility authority.

2.3 System Testing

Upon successful integration of all hardware components, system testing was carried out to assess the performance and verify the functionality of the proposed solution. The testing process involved systematically varying the connected loads and voltage supply to observe the system's real-time response under different operating conditions. Following the experiments, a confusion matrix was utilized as the primary evaluation metric to validate the system's classification performance in distinguishing between authorized and unauthorized load scenarios.

2.3.1 Testing Scenarios

Two different testing scenarios were established, with ten instances comprising both authorised and unauthorised load connections of varying power ratings. This thus provides a comprehensive framework for broad testing of the system sensitivity and its accuracy in detecting bypass incidents on the energy meter.

i. Authorised Load: In five of the instances, different load sizes are connected to the legal load terminal to test the system's response to the authorised energy consumption. While the authorised point is left idle.

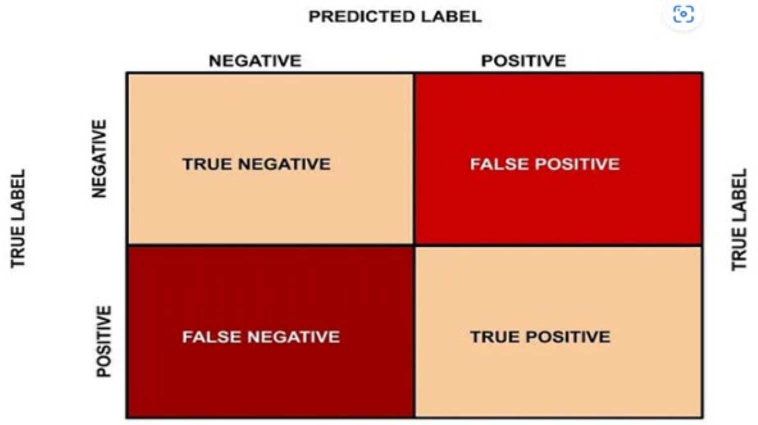
ii. Mixed Loads: The remaining five cases are a combination of legally connected loads and bypass connections.

The investigation checks the accuracy and effectiveness of the detection system, emphasising instances of successful identification of potential electricity theft based on current deviations.

2.3.2 Confusion Matrix

A confusion matrix is a vital metric used to evaluate the performance of a system in classification tasks. It provides insight into the system's ability to correctly distinguish between unauthorised and legitimate loads. Figure 6 presents the confusion matrix used in this study. The True Positive (TP) outcome represents correctly identified electricity theft cases, while the True Negative (TN) refers to correctly identified authorised load conditions. These values indicate the system's effectiveness in detecting theft without misclassifying normal conditions.

On the other hand, both False Positive (FP) and False Negative (FN) outcomes reflect classification errors, highlighting system performance deficiencies. A false positive occurs when an authorised load is mistakenly flagged as theft, resulting in a false alarm. Conversely, a false negative represents a case where the system fails to detect an actual theft, implying poor sensitivity. In such instances, bypass operations succeed undetected.



PREDICTED LABEL

TRUE LABEL	NEGATIVE	POSITIVE
NEGATIVE	TRUE NEGATIVE	FALSE POSITIVE
POSITIVE	FALSE NEGATIVE	TRUE POSITIVE

TRUE LABEL

Figure 6: Confusion matrix label

3.0 Results and Discussion

Figure 7 shows the complete system setup during testing, with incandescent lamps used as test loads. The sensitivity test results are summarised in Table 1, which illustrates the system's capability to identify unauthorised

Received: 02/07/2025; Revised: 07/07/2025; Accepted: 08/07/2025; Published: 08-08-2025

usage of utility power. In Table 1 and Table 2, the Load (W) column denotes the total power consumption connected to the system. The CT1 readings represent the current measured at the utility side (input), accounting for both legitimate and bypassed loads. Conversely, the CT2 readings reflect the current measured at the energy meter, representing the officially recorded consumption.

The system employs a microcontroller to perform a real-time comparison between CT1 and CT2 values. Whenever a significant discrepancy is identified—specifically, when CT1 > CT2—the system interprets this as a theft scenario. Under such conditions, the system automatically flags the event and generates a notification indicating energy theft.

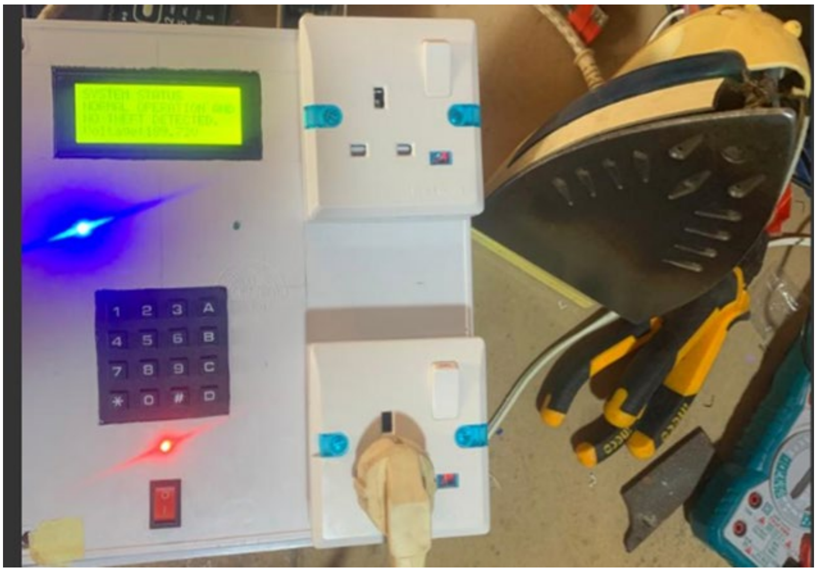


Figure 7: Electricity Theft Detection System Prototype

In Table 1, Cases 1, 3, 5, 7, and 8 displayed equal values for CT1 and CT2, correctly indicating a "No Theft Detected" status. These instances demonstrate the system's capability to differentiate normal electrical usage from potentially fraudulent activities.

Conversely, in Table 2, Cases 2, 4, 6, 9, and 10 exhibited significant discrepancies between CT1 and CT2 values, which were accurately flagged as electricity theft. In these scenarios, the microcontroller initiates communication with the GSM module to notify the utility provider and simultaneously activates the relay to disconnect the power supply. For instance, in Case 4, CT1 measured a current of 1.65 A, whereas CT2 recorded only 0.721 A. This mismatch was interpreted by the microcontroller as a bypass event, prompting the system to trip the relay and transmit a theft alert message via the GSM module.

The overall testing scenario is better illustrated in the bar chart shown in Figure 8. The chart compares CT1 and CT2 readings across all test cases, serving as a visual indicator of theft occurrences. As shown, Cases 1, 3, 5, 7, and 8 are represented with blue bars, indicating that CT1 and CT2 are equal—hence, no theft. In contrast, red and orange bars highlight cases where discrepancies were detected between CT1 and CT2, signifying ongoing electricity theft. This graphical representation enhances the interpretability of the results and provides a clearer understanding of the system's detection performance.

Table 1: System Sensitivity Test Result for the Authorised Case

Case	Voltage(V)	Load (W)	CT1(A)	CT2(A)	Theft Detected	Status Message
1	200	100	0.5	0.5	No	No Theft Detected
3	220	400	1.8182	1.8182	No	No Theft Detected
5	215	800	3.7210	3.7210	No	No Theft Detected
7	210	100	0.5	0.5	No	No Theft Detected
8	230	200	0.8696	0.8696	No	No Theft Detected

Received: 02/07/2025; Revised: 07/07/2025; Accepted: 08/07/2025; Published: 08-08-2025

Table 2: System Sensitivity Test Result for the Mixed Load Cases

Case	Voltage(V)	Load(W)	CT1(A)	CT2(A)	Theft Detected	Status Message
2	210	200	0.9524	0.00	Yes	Disparity Detected! Theft is Ongoing
4	218	360	1.650	0.734	Yes	Disparity Detected! Theft is Ongoing
6	225	400	1.7778	0.888	Yes	Disparity Detected! Theft is Ongoing
9	221	348	1.57	0.834	Yes	Disparity Detected! Theft is Ongoing
10	205	100	0.4878	0.0	Yes	Disparity Detected! Theft is Ongoing

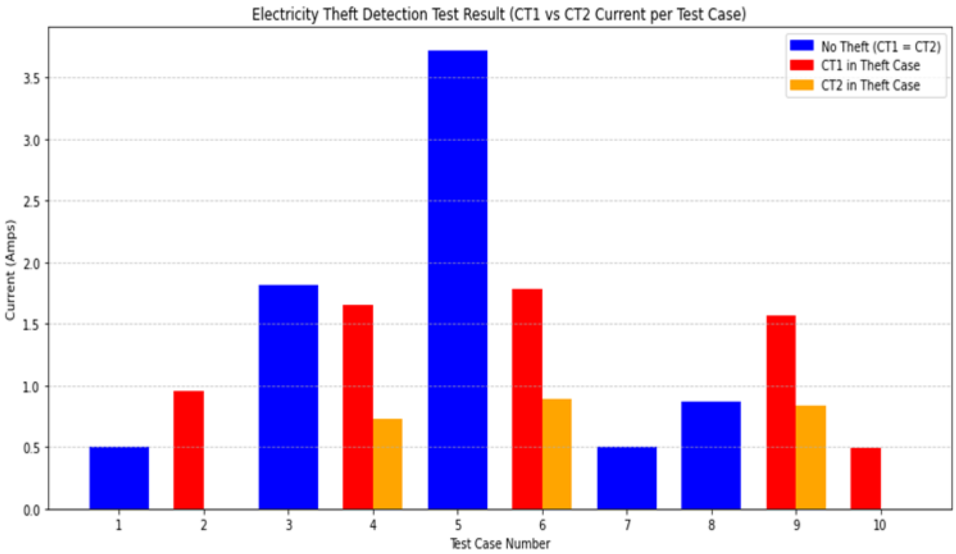
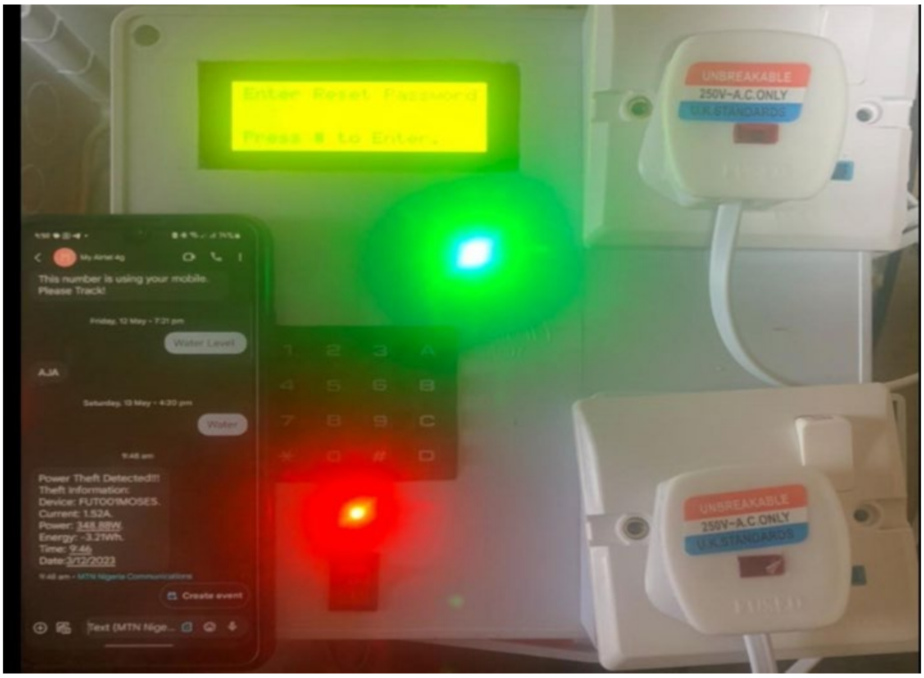


Figure 8: Electricity Theft Detection Comparison Chart

The uniqueness of the system lies in its GSM module, which delivers a detailed theft incident report, as shown in Figure 9; '*Power Theft Detected, Theft Information: Device: FUTOOMOSES, Current: 1.57A, Power: 348w, Energy:3.27wh, Time: 9:46 am, Date: 3/12/2023'*.



This number is using your mobile. Please Track!

Friday, 12 May • 7:21 pm

Water Level

AJA

Saturday, 13 May • 4:20 pm

Water

9:48 am

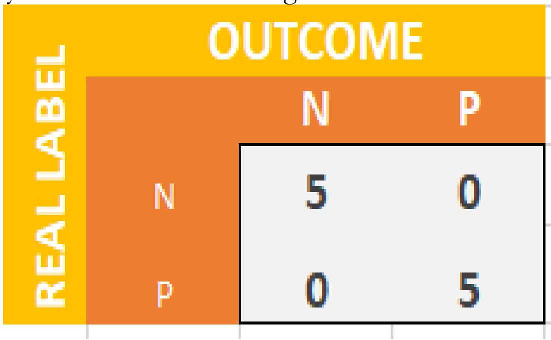
Power Theft Detected!!!
Theft Information:
Device: FUTO01MOSES.
Current: 1.52A.
Power: 348.88W.
Energy: -3.21Wh.
Time: 9:46
Date:3/12/2023

9:48 am • MTN Nigeria Communications

Figure 9: Electricity Theft Detection System Prototype

Received: 02/07/2025; Revised: 07/07/2025; Accepted: 08/07/2025; Published: 08-08-2025

Figure 10 illustrates the theft detection accuracy of the proposed system. The system successfully classified all five authorized load conditions as True Negatives (TN)—indicating no unauthorized consumption—and all five theft scenarios as True Positives (TP), accurately identifying bypass activities. Importantly, there were no occurrences of False Positives (FP) or False Negatives (FN) during testing. As a result, the confusion matrix confirms a 100% detection accuracy, demonstrating the system's high reliability in identifying electricity theft. This complete alignment between expected outcomes and system responses underscores the robustness of the detection mechanism, particularly under controlled testing conditions.



REAL LABEL	OUTCOME	
	N	P
N	5	0
P	0	5

Figure 10: Confusion Matrix

However, while the experimental results are promising, it is essential to acknowledge the potential challenges that may arise in real-world deployment. Factors such as measurement noise, grid fluctuations, and variations in household or industrial appliance behavior could affect detection accuracy. These limitations should be considered when scaling the system for widespread use, and future improvements may include filtering techniques and adaptive thresholds to enhance performance in dynamic environments.

4.0 Conclusion

This project presents a practical and impactful solution for both utility providers and consumers through the development of an Arduino-based intelligent power theft detection system. The system utilizes current sensors and GSM communication to monitor real-time electricity usage, detect anomalies, and relay alerts to utility companies.

In this study, the prototype was rigorously tested across 10 distinct scenarios, covering both authorised and unauthorised load conditions. The system achieved a 100% detection accuracy, correctly identifying all bypass attempts without generating any false alarms. This high performance underscores the system's reliability in enhancing security across power distribution networks, thereby mitigating unauthorised consumption and revenue loss.

Compared to conventional methods, the proposed solution offers a more reliable, cost-effective, and efficient approach to electricity theft detection. The integration of an automated relay further enhances the system by enabling immediate power disconnection in response to theft detection, effectively curbing ongoing illegal usage.

While the system has demonstrated strong performance, certain improvements could further enhance its functionality. One key recommendation is the incorporation of bidirectional communication, which would allow utility providers not only to receive theft alerts but also to remotely disconnect and reconnect power—particularly in cases of repeated theft or non-payment.

Additionally, the current design is tailored for single-phase systems; therefore, future research should focus on extending the system to support three-phase configurations, making it suitable for industrial and commercial applications. These enhancements will improve the system's scalability, adaptability, and overall effectiveness in addressing electricity theft on a broader scale.

References

[1] H. Doukas, C. Karakosta, A. Flamos, and J. Psarras, "Electric power transmission: An overview of associated burdens," *Int. J. Energy Res.*, vol. 35, no. 11, pp. 979–988, 2010, doi: 10.1002/er.1745.

[2] C. L. Zulu and O. Dzobo, "Real-time power theft monitoring and detection system with double-connected data capture system," *Electr. Eng.*, vol. 105, no. 5, pp. 3065–3083, 2023, doi: 10.1007/s00202-023-01825-3.

[3] T. Ahmad, "Non-technical loss analysis and prevention using smart meters," *Renew. Sustain. Energy Rev.*, vol. 72, pp. 573–589, 2017, doi: 10.1016/j.rser.2017.01.100.

[4] M. S. Saeed *et al.*, "Detection of Non-Technical Losses in Power Utilities—A Comprehensive Systematic Review," *Energies*, vol. 13, no. 18, p. 4727, 2020, doi: 10.3390/en13184727.

[5] X. Xia, Y. Xiao, P. Tryjanowski, and J. Cui, "Detection Methods in Smart Meters for Electricity Thefts: A Survey," *IEEE Xplore*, vol. 110, no. 2, pp. 273–319, 2022, doi: 10.1109/jproc.2021.3139754.

[6] A. O. Otuoze *et al.*, "Detection and confirmation of electricity thefts in Advanced Metering Infrastructure by Long Short-Term Memory and fuzzy inference system models," *Niger. J. Technol. Dev.*, vol. 21, no. 1, pp. 112–130, 2024, doi: 10.4314/njtd.v21i1.2294.

[7] P. M. Kgaphola, S. M. Marebane, and R. T. Hans, "Electricity Theft Detection and Prevention Using Technology-Based Models: A Systematic Literature Review," *Electricity*, vol. 5, no. 2, pp. 334–350, 2024, doi: 10.3390/electricity5020017.

[8] P. Jokar, N. Arianpoo, and V. C. M. Leung, "Electricity Theft Detection in AMI Using Customers' Consumption Patterns," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 216–226, 2016, doi: 10.1109/tsg.2015.2425222.

[9] R. E. Ogu and G. A. Chukwudebe, "Development of a cost-effective electricity theft detection and prevention system based on IoT technology," *IEEE*, 2017, doi: 10.1109/nigercon.2017.8281943.

[10] S. Tarafder and K. Banerjee, "Power Theft Detection and Automatic Elimination," *Int. J. Innov. Sci. Res. Technol.*, vol. 4, no.2, 2019, [Online]. Available:https://ijisrt.com/wp-content/uploads/2019/03/IJISRT19FB319.pdf

[11] Z. A. Khan, M. Adil, N. Javaid, M. N. Saqib, M. Shafiq, and J.-G. Choi, "Electricity Theft Detection Using Supervised Learning Techniques on Smart Meter Data," *Sustainability*, vol. 12, no. 19, p. 8023, 2020, doi: 10.3390/su12198023.

[12] Z. Yan and H. Wen, "Electricity Theft Detection Base on Extreme Gradient Boosting in AMI," *IEEE Trans. Instrum. Meas.*, vol. 70, pp. 1–9, 2021, doi: 10.1109/tim.2020.3048784.

[13] L. J. Lepolesa, S. Achari, and L. Cheng, "Electricity Theft Detection in Smart Grids Based on Deep Neural Network," *IEEE Access*, vol. 10, pp. 39638–39655, 2022, doi: 10.1109/access.2022.3166146.

[14] J. Chen, Y. A. Nanehkaran, W. Chen, Y. Liu, and D. Zhang, "Data-driven intelligent method for detection of electricity theft," *Int. J. Electr. Power Energy Syst.*, vol. 148, p. 108948, 2023, doi: 10.1016/j.ijepes.2023.108948.

[15] A. Rauf and A. F. Adekoya, "Systematic literature review of the techniques for household electrical appliance anomaly detections and knowledge extractions," *J. Electr. Syst. Inf. Technol.*, vol.10, no.1,2023,doi: 10.1186/s43067-023-00086-1.

[16] T. P. Ojo, A. O. Akinwumi, F. O. Ehiagwina, J. M. Ambali, and I. S. Olatinwo, "Design and Implementation of a GSM-based Monitoring System for a Distribution Transformer," *Eur. J. Eng. Technol. Res.*, vol. 7, no. 2, pp. 22–28, 2022, doi: 10.24018/ejeng.2022.7.2.2733.

Received: 02/07/2025; Revised: 07/07/2025; Accepted: 08/07/2025; Published: 08-08-2025