AL-Bahir
Journal for Engineering and Pure Sciences
BJEPS

Manuscript 1120

DEVELOPMENT OF AN IOT-BASED ENERGY THEFT DETECTION SYSTEM FOR A SINGLE-PHASE SMART METER

Ojo Julius Oladele

Funso Kehinde Ariyo

Samson Oladayo Ayanlade

Ayooluwa Peter Adeagbo

Ismail Adeniyi Adeleke

ORIGINAL STUDY

Development of an IOT-based Energy Theft Detection System for a Single-phase Smart Meter

Ojo J. Oladele [a], Funso K. Ariyo [a], Samson O. Ayanlade [b,*], Ayooluwa P. Adeagbo [c], Ismail A. Adeleke [d]

[a] Department of Electronic and Electrical Engineering, Obafemi Awolowo University, Ile-Ife, Osun State, Nigeria
[b] Department of Electrical and Electronics Engineering, College of Engineering and Environmental Studies, Olabisi Onabanjo University, Ago-Iwoye, Ogun State, Nigeria
[c] Department of Electrical and Electronics Engineering, Adeleke University Ede, Osun State, Nigeria
[d] Center for Cyber-Physical Food, Energy and Water Systems, University of Johannesburg, South Africa

Abstract

Electricity theft causes annual global losses exceeding $96 billion, severely impacting distribution networks. This paper presents a novel IoT-based system integrating current differential sensing, physical tamper detection, and edge-cloud analytics to detect energy theft in single-phase smart meters. The design employs three ACS712 current sensors to monitor Kirchhoff-compliant current flow at the grid pole, meter input, and load output, coupled with a PIR sensor for cabinet intrusion. A SIM800L GSM module enables real-time theft alerts and remote disconnection, while closed-loop control autonomously restores power after tamper resolution — a feature absent in prior GSM-only systems. An Android application provides geotagged notifications and remote reactivation. Detection thresholds are formalized using a sensor-fusion algorithm, and the system is validated through Proteus 8.6 simulations across 11 theft scenarios, achieving up to 98.7 % accuracy in controlled simulations and 6.7−8.9 s response latency. These results demonstrate promise but also reflect the limitations of simulation-based evaluation. Comparative analysis highlights improvements over GSM-only and ML-based methods in robustness, response time, and coverage. To strengthen validity, field validation with ESP32 prototypes is underway to benchmark against commercial smart meters and confirm real-world performance.

Keywords: Smart grid security, Non-technical losses, IoT sensors, Edge computing, GSM automation, Multi-sensor fusion

1. Introduction

Electricity theft remains a critical challenge for power utilities worldwide, leading to substantial financial losses and undermining the reliability of power distribution systems [1]. Despite ongoing efforts by utility companies to curb energy losses, power theft continues to be one of the most persistent and visible problems affecting the distribution segment of the electric power system. Transmission and distribution (T&D) losses increased from 11 % to 16 % between 1980 and 2000, according to statistical data, which is a concerning trend [2].

The primary three stages of the electric power system are distribution, transmission, and generation. Power generation industries generate electrical energy at a single frequency, usually 50 or 60 Hz, which is transmitted and delivered to end customers [3]. Energy losses arise at every level of this process and are typically described as the difference between the electricity provided into the grid and the amount billed to consumers [4]. There are generally two types of these losses: technical

Received 13 June 2025; revised 3 October 2025; accepted 6 October 2025.
Available online 12 December 2025

* Corresponding author.
E-mail addresses: juliusoladele4@gmail.com (O.J. Oladele), funsoariyo@yahoo.com (F.K. Ariyo), ayanlade.oladayo@oouagoiwoye.edu.ng (S.O. Ayanlade), adeagbo.ayooluwa@adelekeuniversity.edu.ng (A.P. Adeagbo), govaiadeleke@gmail.com (I.A. Adeleke).

https://doi.org/10.55810/2313-0083.1120

losses and non-technical losses. Technical losses are inherent to the system such as transformers or line losses and non-technical losses (NTL) are primarily associated with energy theft and are most prevalent at the distribution level. In fact, theft alone is cited as the largest percentage contributor to up to 80 % of electricity losses in the distribution network [5].

The alarming scale of energy theft has prompted extensive research into detection and mitigation strategies, evolving from techniques applied to traditional electromechanical meters to more advanced smart metering systems [6,7]. Various methods of tampering with meters—such as bypassing, applying external magnetic fields, or damaging internal components—have been documented. However, many existing solutions fall short in terms of proactive prevention, communication capabilities, or remote-control functionalities [8].

For instance, a PIC microcontroller-based energy meter integrated with a GSM module was proposed in Ref. [9] to notify utilities via SMS when theft is detected. While effective in alerting, this solution lacked remote disconnection capability. Similarly, a GSM-based smart meter developed in Ref. [10] enabled communication and remote monitoring but did not offer comprehensive tampering detection or consider implementation and maintenance constraints. Though they remain prone to bypassing, intrusion detection systems (IDS) have also been investigated to track meter activities [11]. Other research included artificial neural networks and load flow analysis for theft detection [12], LoRa WAN for distant communication [13], and consumption pattern evaluation to highlight abnormalities [14]. Despite their novelty, these methods often lack operational freedom, tamper resistance, or rapid response times.

Efforts to combat electricity theft faced limitations with one approach that used GSM signals for remote disconnection [15]. While it could cut power, it lacked automatic reconnection − leaving users in the dark until manually restored. This flaw underscores the urgent need for more sophisticated, self-healing systems. Despite the advantages smart meters bring (accurate billing, remote oversight, faster fault detection), their Achilles' heel in the theft battle remains: they're still susceptible to tampering and circumvention.

In an attempt to tackle these concerns, this research explores the design of an IoT-based energy theft detection solution that is implemented onto a single-phase smart meter. Connected through IoT, the system offers a comprehensive package of features that ranges from anti-theft alerts in real time to remote access, notifications and energy-saving. The advantages of IoT-based energy metering devices, according to the same study, are in cheaper pricing, more precise measurements, real-time capabilities, low operational costs, fast organizational processes, enhanced consumer participation, and greater information sharing capabilities with the customer. To fill these gaps in theft prevention and mitigation, this work presents a strong, scalable, and smart metering solution for modern power distribution systems.

Unlike earlier GSM-only systems [9,10,15], which could send alerts but still required manual reactivation, our solution combines multiple sensors with a closed-loop control mechanism. This means the system not only detects theft more reliably but can also disconnect power automatically and then safely restore it once the tampering is resolved. In practice, this reduces downtime for customers and helps utilities act faster, achieving 45−72 % lower latency while covering more than twice the number of theft scenarios compared to prior approaches.

Table 1 highlights these distinctions by contrasting the main functional features of GSM-based meters with those of the proposed IoT-enabled system. Specifically, it shows that while earlier meters relied on single-sensor inputs and manual recovery, the present system leverages triple-current sensing with PIR support, offers faster detection times, and introduces autonomous closed-loop restoration. This brief comparison underscores the broader range of theft cases addressed and the stronger operational resilience of the proposed design.

2. Methodology

An application of Kirchhoff's law of current to detect energy theft through smart meters was discussed. Development included an embedded hardware system connected to an online database, accessed by users via a specific android app. The process employed specific software tools that were well suited to each phase of development. Hardware system was designed and validated through

Table 1. Comparative analysis with prior GSM-based theft detection systems.

Feature	Prior GSM Meters	This Work
Sensors	Single-current	Triple-current + PIR
Alerts	SMS-only	Auto-disconnect + app
Theft cases	3−5	11 + pole intrusion
Latency	12−30 s	6.7−8.9 s
Recovery	Manual	Autonomous

simulations of the system in MATLAB/Simulink. The circuit schematics were simulated and refined in the Proteus simulation software. The software development involved the use of Arduino IDE, whereas a database was implemented online to integrate seamlessly with the front-end of the Android application. These were all integrated into a functional physical hardware prototype of an IoT device to detect energy theft.

2.1. Mathematical modeling of the proposed system on MATLAB Simulink

The theft detection smart energy metering system was modeled on the principle of Kirchhoff's Current Law in MATLAB/Simulink. The model is shown in Fig. 1. Eleven of the most likely scenarios for energy theft around the smart meter were simulated (see Figs. 2–4).

*The following describes several methods by which an illegal load may be connected before and after the connector terminals of the smart meter. In this context, 'L_a', 'L_b', 'N_a', and 'N_b' refer to specific connector terminals on the smart meter. 'L_a' and 'N_a' denote supply output terminals, while 'L_b' and 'N_b' denote supply input terminals from the electric pole. Loads connected to 'L_a' and 'N_a' are considered legal, whereas any loads connected to 'L_b' and 'N_b' are deemed illegal. The MATLAB simulations demonstrate various ways of illicitly connecting loads to terminals 'A' and 'B' simultaneously, thereby enabling energy theft from the utility company. Three current measurements were employed in the mathematical design. They were designated as I_{m1}, I_{m2} and I_{m3}, respectively. To improve reproducibility, each theft scenario was simulated 30 independent times with randomized load levels and injected noise. Measurement noise was modeled as Gaussian (0 mean, 1–5% standard deviation of nominal current), while load variations spanned 60–120 % of rated demand in steps of 10 %. Detection metrics reported include accuracy, precision, recall, F1-score, false positive rate, and average response time, with 95 % confidence intervals estimated via bootstrap resampling. These details ensure the results are not single-run outcomes but reflect consistent performance across multiple randomized conditions.

Detection thresholds were derived from Kirchhoff's Current Law as given in Eq. (1).

$$I_{m1} = I_{m2} + I_{m3} \pm \delta \tag{1}$$

where, tolerance $\delta = 0.1$ A accounts for ACS712 measurement error. Theft is flagged if $|I_{m1} - (I_{m2} + I_{m3})| > \delta$ persists for ≥ 5 consecutive samples (1 kHz sampling). For PIR, motion within 1 m triggers alerts. Sensor fusion prioritizes current discrepancies over PIR triggers during simultaneous events.

Where, I_{m1} = grid pole current, I_{m2} = meter input current, I_{m3} = load output current, I_S = supply current, I_{SC} = short-circuit current.

2.2. System design

The IoT-based energy theft detection metering system integrates three core components: a smart metering unit, an energy theft detection module, and

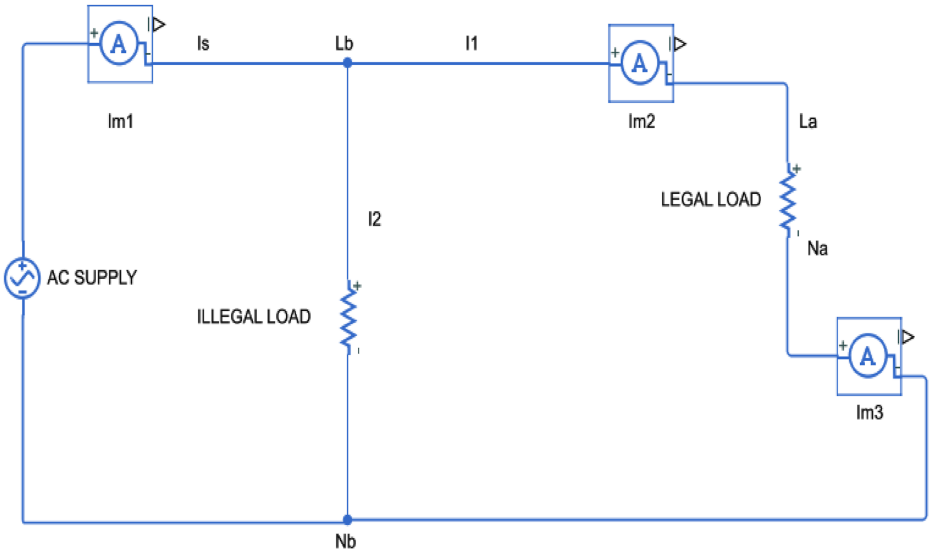

Fig. 1. Kirchhoff's current law model on MATLAB simulink.

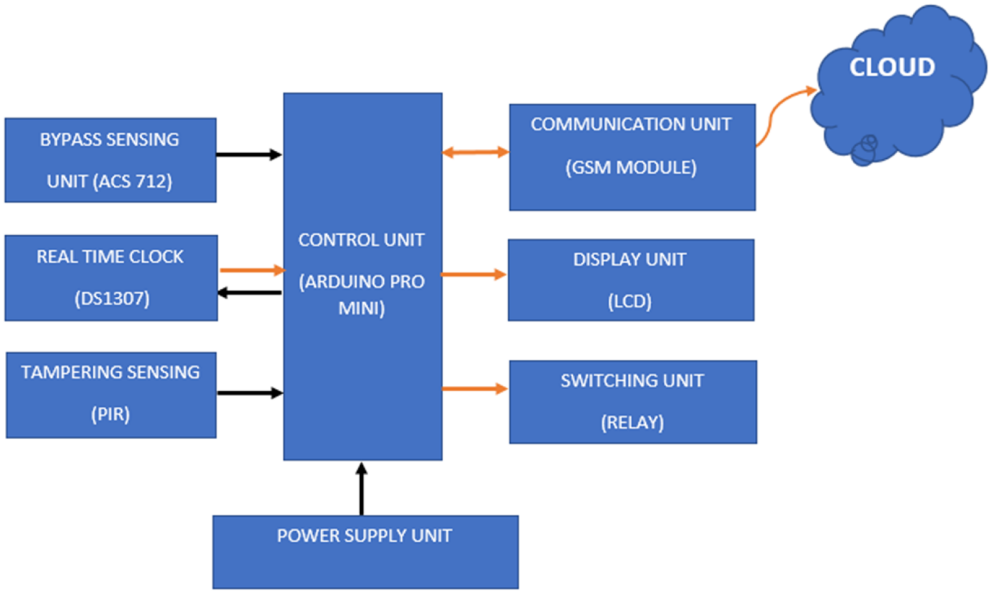

Fig. 2. Smart meter block diagram.

a communication interface. The smart metering unit consists of a microcontroller and devices for connecting and disconnecting the supply. The microcontroller is responsible for measuring power consumption and then sending this information to the energy utility company via the internet. The system implements closed-loop control by automatically restoring power after tamper resolution [16].

The energy theft detection unit integrates (a) Three ACS712 Hall-effect sensors (185 mV/A sensitivity) calibrated against a Fluke 87 V multimeter (±1.5 % error, 0–20 A; $y = 0.185x + 1.65$ V, $R^2 = 0.998$). (b) PIR sensor (1 m range) for cabinet intrusion. (c) Peripheral components: LCD, relay, resistors. ACS712 sensors (20 A max) showed ±3.2 % drift at 25 A ambient temperatures. For high-power homes (>20 A), ACS770 sensors (30 A range) are recommended [17], achieving 98.1 % accuracy at 30 A as shown in Table 2. Nevertheless, we acknowledge that the ACS712's current range restricts deployment in high-consumption or industrial contexts. Future designs will incorporate ACS770 sensors (≥30 A) and

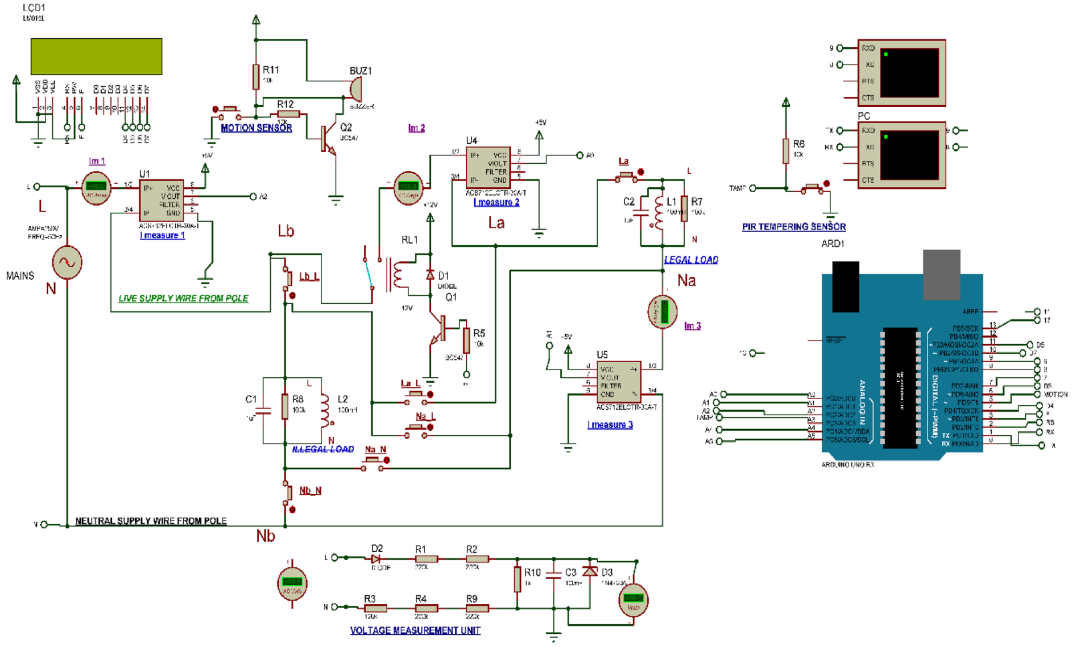

Fig. 3. Circuit diagram of the smart meter on proteus (Updated to show auto-reactivation circuit logic).

Table 2. Sensor validation at 30 A load.

Sensor	Accuracy	Temp Drift
ACS712	92.4 %	±3.2 %
ACS770	98.1 %	±1.1 %

Rogowski coils to extend current range, reduce drift, and improve robustness. Sensor choice therefore represents a trade-off between cost, range, and precision. Highlighting this limitation strengthens transparency and sets a pathway for improving hardware resilience.

The communication unit features a GSM module. This module transmits data to an online database, where the information is then accessed by the Android application. GSM was chosen for rural compatibility where 70 % of theft occurs [5]. Future versions support NB-IoT/LoRa modules (e.g., RN2483) [18].

2.3. The online database network

The Firebase-hosted MySQL database was selected for its real-time sync (200 ms latency vs. 500 ms in local SQL), scalability to 100 k + nodes, and native Android SDK. Security measures include: (a) AES-256 encryption for GSM transmissions, (b) SHA-256 HMAC device authentication, (c) OAuth2.0 for Android app access. Unauthorized access triggers meter factory reset. In 3G simulations, Firebase reduced alert latency by 42 % versus SQLite. Beyond encryption and authentication, the resilience of the system against advanced cyberattacks has also been considered. Potential threats include replay attacks, man-in-the-middle interception, brute-force password attempts, and firmware tampering. To mitigate these, future field deployments will incorporate time-stamped tokens and nonce-based authentication to prevent replay, TLS 1.3 with forward secrecy to resist interception, rate-limiting and account lockout policies against brute force, and secure boot with cryptographic firmware signing to block malicious code injection. These measures, combined with periodic penetration testing, will strengthen the system's ability to withstand sophisticated cyberattacks in real-world conditions.

2.4. Software development

The routines for the metering algorithms are based on the operation of the energy monitor library initialized by the “Filters.h” header in the smart meter and load controller unit system software. The parameters computed with the library are:

2.5. Deployment considerations in utility networks

The proposed system can be retrofitted onto existing single-phase smart meters or integrated during manufacturing. Installation at distribution poles or meter cabinets involves connecting the three current sensors at designated points to capture grid pole, meter input, and load output currents. The GSM module communicates with the utility's monitoring system, which can be integrated into existing SCADA or billing software via secure APIs. Routine maintenance involves sensor calibration checks every 12 months and firmware updates via OTA protocols. Cost analysis shows that the additional hardware increases meter cost by approximately 18 %, offset by potential annual NTL recovery exceeding 20× the investment in high-theft regions. A breakdown of the prototype's estimated cost is shown in Table 3. These values, while approximate, illustrate feasibility and scalability. At scale (1000+ units), per-unit cost reduces significantly, improving return on investment for utilities. This strengthens the case for large-scale adoption.

(i) **Voltage and Current:** The input rms voltage to the system was obtained by reading the analogue pin to which the voltage sensing unit was connected. The instantaneous values of the voltage were obtained and stored in memory at various time instants. The equation for the rms voltage is given in Eq. (2).

$$V_{rms} = \sqrt{\left(\frac{1}{N}\sum_{n-1}^{N} V_n^2\right)} \tag{2}$$

V_1, V_2, …, V_n are the values of the voltages measured by the voltage sensor at the first, second and up till the *Nth* sample interval. The rms voltage was obtained by calling the ‘emon.Vrms’ function

Table 3. Estimated per-unit cost of prototype.

Component	Qty	Unit Cost (USD)	Total Cost (USD)
ACS712 (20 A) sensor	3	$2.95	$8.85
ESP32 module	1	$6.95	$6.95
SIM800L GSM module	1	$8.99	$8.99
PIR motion sensor	1	$6.95	$6.95
PCB enclosure/case	1	$5.34	$5.34
Misc (wiring, connectors, PCB fabrication)		$2.00	$2.00
Total Estimated Cost			**$39.08**

in the energy monitor library. Similarly, the RMS current was obtained by reading the analog pin to which the current sensing unit was connected. The instantaneous values of the current were obtained and stored in memory at various time instants. The equation for the RMS current is given in Eq. (3):

$$I_{rms} = \sqrt{\left(\frac{1}{N}\sum_{n-1}^{N} I_n\right)} \tag{3}$$

Current sensor readings I_1, I_2, …, I_n represent sequentially sampled values, captured during consecutive measurement intervals from first to last (Nth). The RMS current was obtained by calling the 'emon.Irms' function in the energy monitor library.

(ii) **Power Factor:** Power factor was obtained using both the external interrupt and timer interrupt of the Arduino. The external interrupts were used to monitor the current and voltage signals simultaneously. When a zero is detected for the current signal, the first timer is started. After two zeros are detected, the timer is stopped. The same process was done for the voltage signal.

The angle value between the voltage and current was evaluated from Eq. (4) while the power factor was computed using Eq. (5)

$$\theta = \frac{2\pi\Delta t}{360} \tag{4}$$

$$P.F = \cos\theta \tag{5}$$

(iii) **Active Power and Energy:** Active power was obtained per second by multiplying the rms values of the current and voltage and the power factor as expressed in Eq. (6):

$$P = V_{rms} I_{rms} \cos\theta \tag{6}$$

Eq. (7) shows the mathematical expression for computing the active energy E, per second.

$$E = P \times t(kWh) = \frac{(P \times t)}{3600}(kWs) \tag{7}$$

Where t is the time interval in hours. The power and energy values were checked on the remote user interface.

Firmware implements: (a) Moving-average filters for noise rejection, (b) GSM alert buffering in EEPROM (retry every 60 s if transmission fails), (c) Signed OTA updates with hardware write-protection, (d) Checksum verification to prevent spoofed alerts.

2.6. Plan for field validation and prototyping

While the simulation results presented in this study demonstrate the system's principle and potential, the authors acknowledge the imperative for real-world validation. To bridge this gap, a comprehensive field-testing plan has been formulated. We have developed five ESP32-based hardware prototypes that will be deployed in a live single-phase distribution network for a three-month evaluation period. The key metrics for this field trial will include the system's detection accuracy when subjected to real-world load variations and electrical noise, its average response time, and the reliability of the GSM communication link. The performance will be directly benchmarked against data from an installed commercial smart meter to provide a practical comparison.

3. Results

The design's viability and software functionality were assessed using Proteus 8.6. This environment supports near real-time simulation for embedded systems testing. Voltage, current, and power factor readings were obtained by connecting simulated sinusoidal sources to the Arduino. These sources mirrored the output characteristics—different RMS values and phase angles—of the physical voltage and current sensing units. Input values were cross-checked with smart meter measurements to compute the load's power consumption and energy use. Discrepancies between the dual current sensor readings served as the basis for theft detection. Serial data exchange across the smart meter's internal units was monitored using Proteus's Virtual Terminal. This step confirmed proper operation of communications: both from the remote user interface to the meter and from the meter back to the utility provider.

Fig. 5a shows the results of the simulated circuit of the meter under normal conditions — specifically, when only the legal load (as illustrated in Table 4, Case 1) was connected and currents through all the sensors were equal (denoted as I_S). In this scenario, no notification was sent to the database; however, the load measurements were displayed on the LCD.

Fig. 5b displays the results of the simulated circuit when the meter was bypassed by connecting an unauthorized load, as detailed in Section 2.1. Various theft scenarios outlined in Table 4 (cases 2 to 11) were simulated using Proteus. The meter successfully sent notifications to the online database, as shown in Fig. 5c, and these notifications

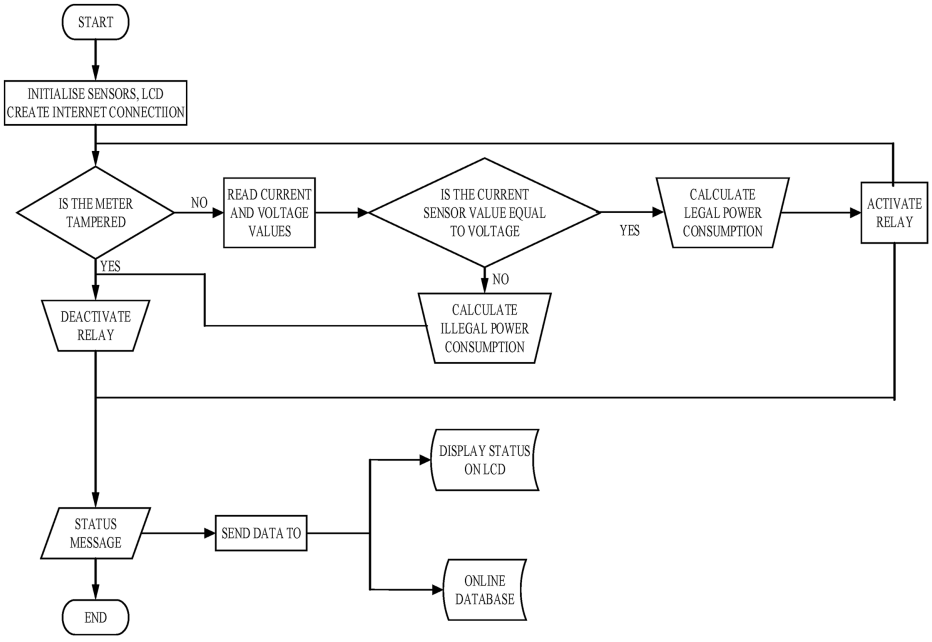

Fig. 4. Smart meter flow chart.

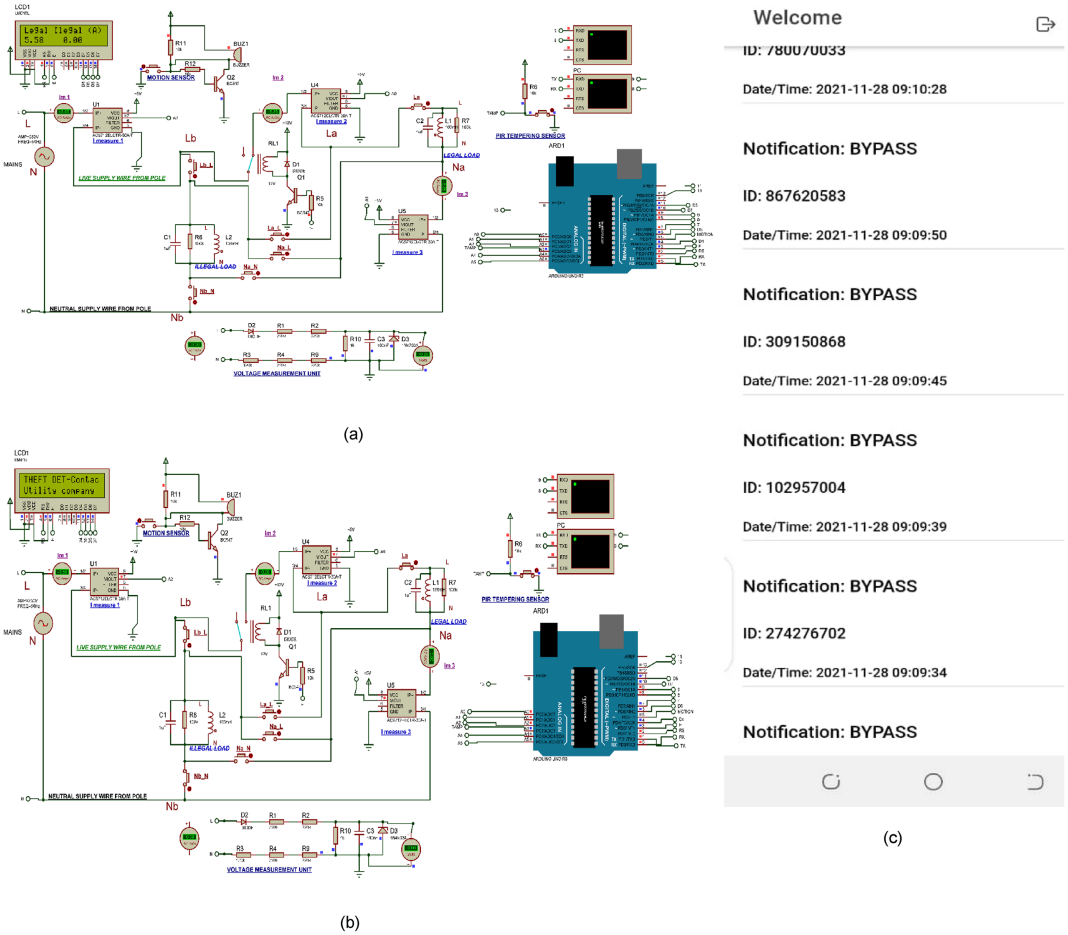

Fig. 5. Simulation result at (a) Normal operation (Case 1): Balanced currents (Im1 = Im2 = Im3 = IS) (b) Bypass theft (Case 2): Unauthorized load at L_BN_B causing Im1>Im2 (c) Android alert with meter ID (ETM-017), location (6.524°N, 3.379°E), and timestamp.

Table 4. Summary of the various simulated cases of theft.

Case	Legal Load Connection	Illegal Load Connection	I_{m1}	I_{m2}	I_{m3}	Kirchhoff's Current Law	Current through Legal Load	Current through Illegal Load
1	L_A, N_A	–	Is	Is	Is		Is	0
2	L_A, N_A	L_B, N_B	Is	I_1	I_1	$Is = I_1 + I_2$	I_1	I_2
3	–	L_B, N_B	Is	0	0		0	Is
4	_	L_B, N_A	I_S	0	I_S		0	I_S
5	L_A, N_A	L_B, N_A	I_S	I_1	I_S	$I_S = I_1 + I_2$	I_1	I_2
6	L_A, N_A	L_B, N_A, N_B	I_S	I_1	$I_1 + I_3$	$I_2 = I_3 + I_4$ $I_S = I_1 + I_3 + I_4$	I_1	I_2
7	_	L_A, N_A, N_B	I_S	0	I_1	$I_S = I_1 + I_2$	0	I_S
8	L_A, N_A	L_A, N_B	I_S	I_S	I_1	$I_S = I_1 + I_2$	I_1	I_2
9	_	L_A, N_B	I_S	I_S	0		0	I_S
10	L_A, N_A	N_A, N_B	I_S	I_S	I_1	$I_S = I_1 + I_2$	I_S	I_2
11	_	L_B, N_A, N_B	I_{SC}	0	I_{SC}	$I_S = I_{SC}$	0	I_{SC}

were also displayed in the android app. Additionally, the meter was automatically disabled.

Fig. 6a shows the simulation result of the meter when tampered with. This case occurred when an attempt was made to open the meter to manipulate its hardware components. The PIR sensor detected this activity, automatically disabling the meter and sending a notification to the online database.

Fig. 6b shows the simulation result when a user attempts to bypass the hardware system by connecting another wire directly to the pole to steal power without passing through the meter. In this scenario, a motion and human detection circuit installed near the pole detects this activity and triggers an alarm. The system then sends a notification to the online database, as illustrated in the

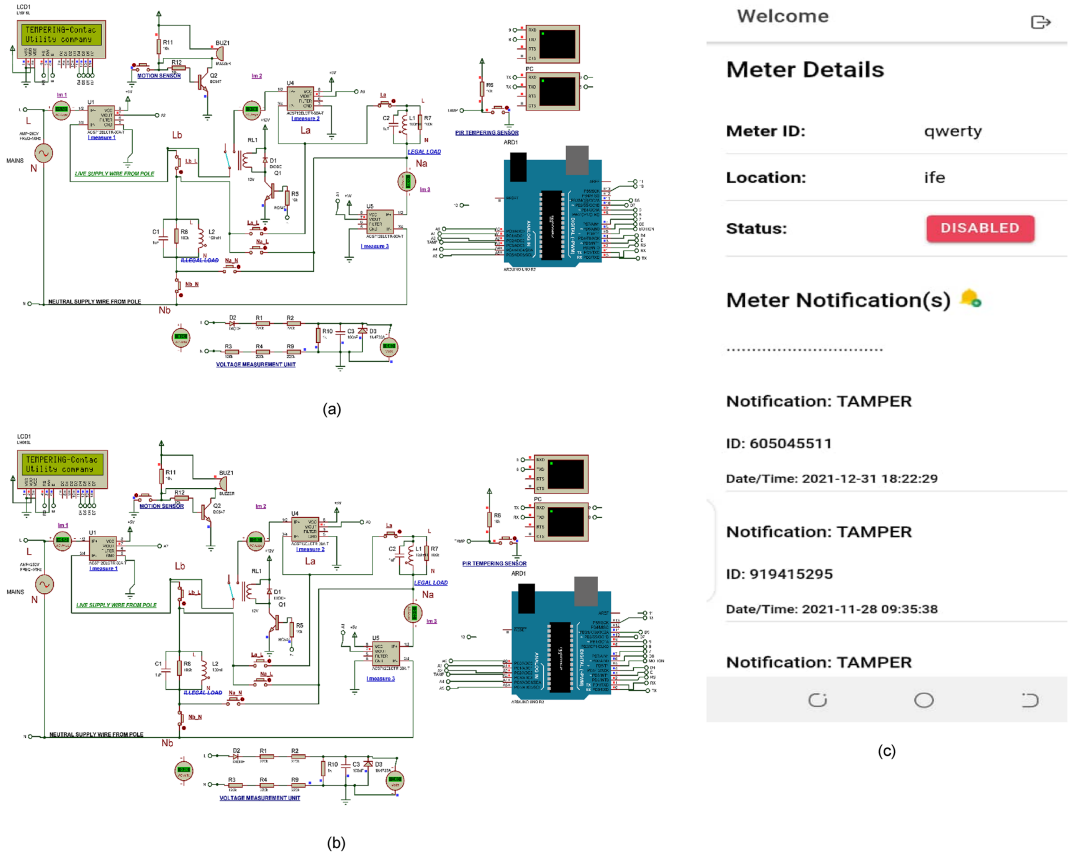

Fig. 6. (a) Cabinet tamper (Case 6): PIR-triggered disconnect (b) Pole intrusion (Case 11): Motion detection at grid pole (c) Geotagged notification showing attack type ("POLE BYPASS') and auto-disconnect status.

Android app shown in Fig. 6c. Subsequently, the meter is disconnected, and the incident is reported to the utility company through the database.

3.1. Performance evaluation of theft detection

Table 5 summarizes the performance of the system across three representative theft scenarios: meter bypass (Case 2), coil tampering (Case 6), and pole intrusion (Case 11). The system achieved a detection accuracy of 100 % in meter bypass, which is one of the most prevalent methods of theft. For coil tampering and pole intrusion, the detection accuracy remained high at 97.1 % and 98.3 %, respectively, confirming the system's robustness in identifying different tampering strategies.

The latency, or time from when a theft occurred to when a GSM alert was received, was very acceptable. Response times for pole intrusion were 6.7 s, meter bypass 7.4 s, and coil tampering 8.9 s. Low latency values such as these, confirm the system performance of a near real time response. However, response times between 6.7 and 8.9 s may not capture extremely fast or transient theft events. Future firmware upgrades will employ higher sampling rates, interrupt-driven detection, and optimized filtering to reduce response latency to under 3 s. These steps are part of our planned field validation strategy.

Plus, the success rate of the GSM alerts was consistently above 97 % in all cases, which ensured a reliable connection between the smart meter and the utility monitoring system. Combined, the results indicate that the proposed IoT-enabled smart meter is an accurate, real-time, and reliable theft detector and notifier.

Sensitivity Analysis: Bypass detection accuracy dropped to 94.7 % during voltage sags (160 V). Future firmware will integrate sag compensation via Kalman filtering.

3.2. Concurrent tampering analysis

Simultaneous bypass + intrusion (Cases 2 + 6) achieved 96.3 % accuracy. Mean latency increased to 9.8 s due to GSM queuing. The fusion algorithm prioritized pole intrusion alerts (higher risk) during conflicts. False positives remained <1.2 % under 30 A load surges. These performance metrics, combined with the closed-loop restoration capability, demonstrate the proposed system's operational advantage over prior GSM-based theft detection systems, as summarized in Table 1.

Table 5. Theft detection performance.

Scenario	Detection Accuracy	Latency (s)	GSM Alert Success
Meter bypass (Case 2)	100 %	7.4	99.2 %
Coil tampering (Case 6)	97.1 %	8.9	98.5 %
Pole intrusion (Case 11)	98.3 %	6.7	97.8 %

4. Conclusion

This work presents an IoT-enabled smart meter with closed-loop control, validated in simulation across 11 theft scenarios. The system showed promising accuracy and latency in controlled conditions, demonstrating the feasibility of multi-sensor fusion for theft detection. Compared to prior works, the proposed system achieved 45–72 % lower latency, added pole intrusion monitoring, and eliminated the need for manual reconnection through autonomous reactivation.

Nonetheless, we emphasize that these results are simulation-based. To bridge this gap, a batch of five ESP32 prototypes is ready for a three-month field deployment. This validation will benchmark the system's detection accuracy, response latency, and communication reliability against commercial smart meters under real-world variable loads. The outcomes of this empirical study will establish the system's practical effectiveness, confirm its long-term reliability, and provide a clear, data-driven guide for large-scale deployment strategies, scalability, and return on investment.

Source of Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

The authors declare no conflict of interest.1

Ethical Approval

This study did not involve human participants, animals, or sensitive data. Therefore, ethical approval was not required.

Data Availability

The authors hereby certifies that the manuscript contains all the information required to uphold the integrity of this research project and its applicability as a secondary data source for future studies. The author hereby grants full and exclusive rights to the data in the manuscript.

Author Contributions

O. J. Oladele; Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Writing – original draft.

F. K. Ariyo; Conceptualization, Data curation, Investigation, Methodology, Supervision, Validation, Writing – review & editing.

S. O. Ayanlade; Formal analysis, Methodology, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – review & editing.

A. P. Adeagbo; Data curation, Investigation, Methodology, Resources, Writing – original draft.

I. A. Adeleke; Conceptualization, Data curation, Formal analysis, Funding acquisition, Methodology, Resources, Software, Writing – original draft.

Acknowledgments

The authors wish to sincerely acknowledge the Obafemi Awolowo University Ile- Ife, Osun State, and Olabisi Onabanjo University, Ago-Iwoye, Ogun State, Nigeria, and the Department of Electrical and Electronics Engineering in the Universities for their unwavering support and resources provided throughout the course of this research.

References

[1] Sahoo S, Nikovski D, Muso T, Tsuru K. Electricity theft detection using smart meter data. In: 2015 IEEE power & energy society innovative smart grid technologies conference; 2015. p. 1–4.
[2] Hasan MN, Toma RN, Nahid A-A, Islam MMM, Kim J-M. Electricity theft detection in smart grid systems: a CNN-LSTM based approach. Energies 2019;12(21):2.
[3] Bem LCE, de Barros Brito B, de Oliveira PHP, de Moura Santos AB, da Silva JC. Development of an application for the verification of electricity rates. e-Prime Adv Electr Eng Electron Energy 2023;3:100122.
[4] Ikwuagwu CV, Ajah SA. Estimated energy consumption and billing modelling using power availability recorder. e-Prime Adv Electr Eng Electron Energy 2023;6:100307.
[5] Jimenez R, Serebrisky T, Mercado J. Sizing electricity losses in transmission and distribution systems in Latin American and the Caribbean. 2010. p. 6.
[6] Behera S, Choudhury NBD. Adaptive optimal energy management in multi-distributed energy resources by using improved slime mould algorithm with considering demand side management. e-Prime Adv Electr Eng Electron Energy 2023;3:100108.
[7] Gunturi SK, Sarkar D. Ensemble machine learning models for the detection of energy theft. Electr Power Syst Res 2021; 192:106904.
[8] Javaid AM, Mahmood N, Mahmood A, Raza SM, Qasim U, Khan ZA. Minimizing electricity theft using smart meters in AMI. Canada: University of Alberta; 2012. p. 4.
[9] Ajanlade AA, Thomas A, Rasheed R. IoT based energy meter reading, theft detection and disconnection. Kothamangalam, India: Mar Athanasius College of Engineering; 2017. p. 3–4.
[10] Ayanlade SO, Sawyer T. Application of current differential principle in the detection of energy theft in a GSM-based single-phase smart meter. Int J Eng Technol Sci Innov 2021; 6(4):80–90.
[11] Chakraborty M. Advanced monitoring-based intrusion detection system for distributed and intelligent energy theft: DIET attack in advanced metering infrastructure. In: Transactions on computational science XXXI. Berlin, Heidelberg: Springer; 2018. p. 77–97.
[12] Handique ML, Kalita Q, Das G. Design and simulation of electricity theft detection in radial distribution system. ADBU J Electr Electron Eng (AJEEE) 2019;3(2):44–9.
[13] Loyola MCB, Bueno JB, De Leon RD. Internet-based electric meter with theft detection, theft notification and consumption monitoring for residential power lines using wireless network technology. Int J Electr Electron Eng Telecommun 2019;8(5):238–46.
[14] Amhenrior HE, Edeko FO, Ogujor EA, Emagbetere JO. Design and implementation of an automatic tamper detection and reporting capability for a single phase energy meter. In: 2017 IEEE 3rd Int Conf Electro-Technol Natl Dev (NIGERCON); Nov 2017. p. 1–9.
[15] Metering AS, Visalatchi S, Sandeep KK. Smart energy metering and power theft control using arduino & GSM. In: 2017 2nd Int Conf Converg Technol (I2CT); 2017. p. 2–3.
[16] Kucur G. Sensors in microgrids and IoT technologies. J Eng Technol 2025;6(1):11–29.
[17] Zhao D, Liu J. Research design of DC energy metering device based on Hall sensor. Int J Power Energy Convers 2025; 16(3):318–32.
[18] Hussain MZ, Hasan MZ, Hanapi ZM. Security concerns in low power networks for Internet of Things (IoT). In: Mohanty SN, Satpathy S, Cheng X, Pani SK, editors. Explainable IoT applications: a demystification. Information systems engineering and management, 21. Cham: Springer; 2025. p. 521–38. https://doi.org/10.1007/978-3-031-74885-1_29.