Iot-Enabled Current–Differential Analytics for Electricity Meter Bypass Detection in Low-Voltage Distribution Systems

J. K. Annan[1*], L. Eshun[2]

[1]Electrical and Electronic Engineering Department, University of Mines and Technology, Tarkwa, Ghana

[2]Electrical and Computer Engineering Department, University of Memphis, Memphis, USA

***Corresponding Author**

DOI: https://dx.doi.org/10.51584/IJRIAS.2025.10120015

Received: 16 December 2025; Accepted: 23 December 2025; Published: 02 January 2026

ABSTRACT

Electricity theft remains a critical challenge for power utilities, particularly in developing economies where non-technical losses significantly disrupt revenue recovery and system reliability. Meter bypassing, where consumers divert current away from the energy meter, is the most pervasive form of electricity theft in Ghana. This study develops and evaluates a conceptual Internet of Things (IoT)-based monitoring system designed to detect meter bypass using a dual current-sensing architecture. The system employs two ACS712 Hall-effect current sensors, an ATmega328p-PU microcontroller, a SIM800A GSM module for SMS alerts, and an ESP8266 WiFi module for cloud-based reporting to the ThingSpeak® platform. Detection relies on a real-time current-difference algorithm that compares load and meter currents within a mathematical tolerance threshold. Simulation using Proteus 8.3 and prototype implementation confirm that the system accurately detects bypass conditions and enables remote disconnection of supply. This research demonstrates a scalable approach for reducing non-technical losses in low-voltage networks.

Keywords: Electricity Theft, Energy Meter, Micro controller, Meter Bypass, IoT, Tampering.

INTRODUCTION

Electricity metering represents the primary interface between utility providers and consumers, ensuring accountability, revenue protection, and system reliability. Although energy meters are installed at consumer premises, ownership typically remains with the utility provider (Fig. 1), forming a legally protected boundary between the distribution network and customer installations. Despite continuous advancements from electromechanical meters to advanced smart metering infrastructure, electricity theft persists as a significant challenge to distribution utilities worldwide.

In Ghana, non-technical losses, largely attributed to theft, meter tampering, and illegal connections, account for approximately 30% of distributed electrical energy (Yakubu *et al*., 2018). Meter bypassing remains the most prevalent technique due to its ease of execution and minimal need for specialized equipment. Conventional inspection-based detection methods are labour-intensive, inefficient, and reactive rather than preventive.

Recent research have explored IoT-based monitoring, machine learning algorithms, and advanced data analytics for theft detection (De Souza *et al*., 2022; Alfriehat *et al*., 2024). However, many existing approaches suffer from high computational complexity, dependence on large datasets, high deployment cost, and limited suitability for retrofitting in legacy low-voltage networks.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XII December 2025

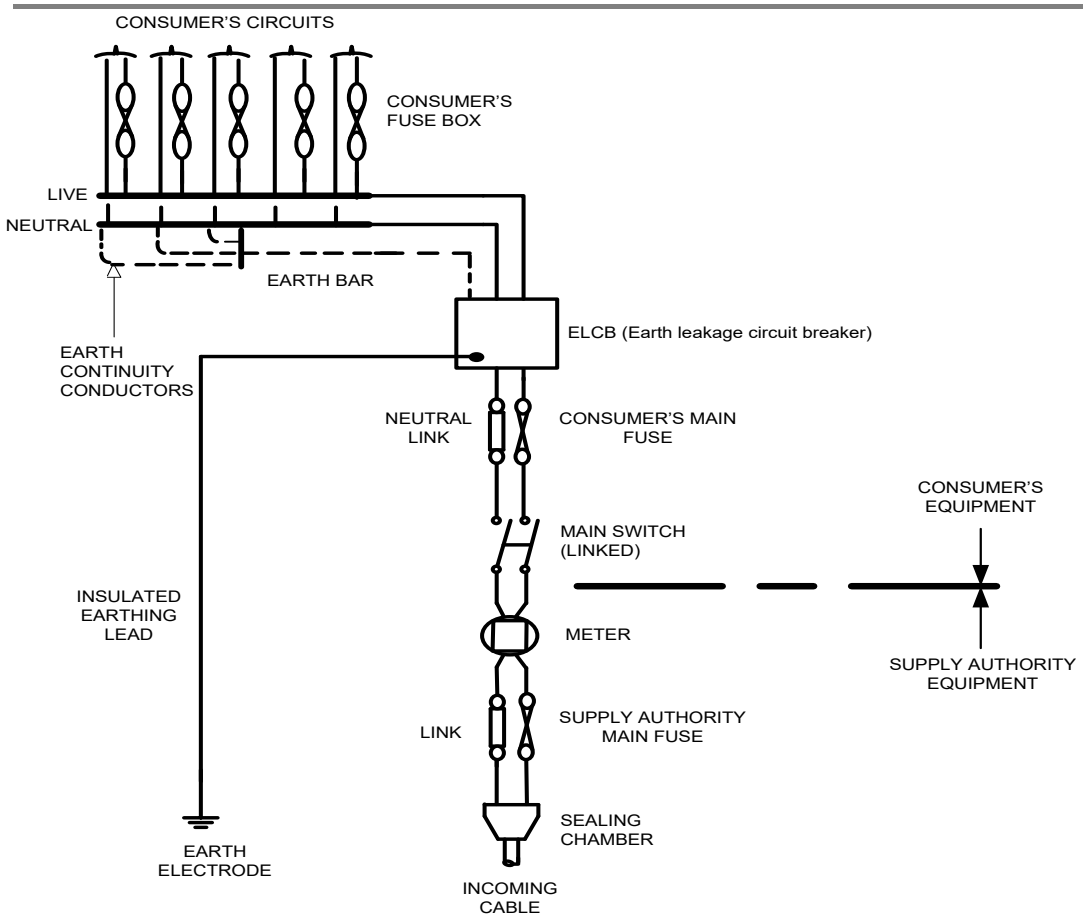

Fig. 1 Equipment at the Supply Point of a Single Phase Domestic Consumer

Fig. 2 shows a basic classification of the energy meter based on factors such as construction, display, phase and billing type.

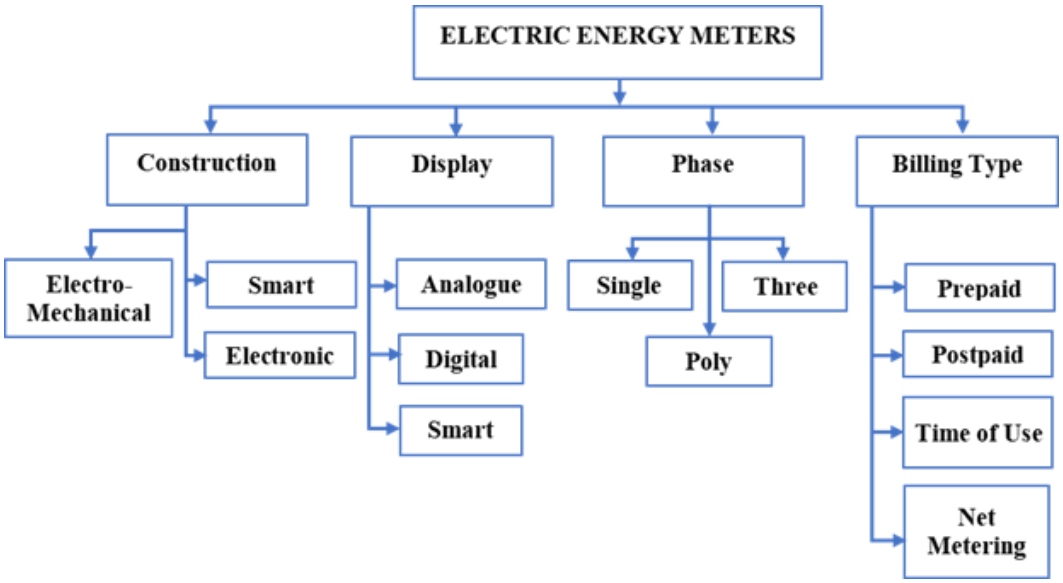

Fig. 2 Basic Classification of Energy Meters

LITERATURE REVIEW

Electricity theft detection techniques broadly fall into hardware-based, data-driven, and hybrid approaches. Hardware-based methods include magnetic field detection, voltage imbalance monitoring, and current imbalance analysis (Tangsunantham *et al*., 2013; Czechowski and Kosek, 2016). Data-driven approaches

utilise artificial intelligence and machine learning models trained on large consumption datasets (Yao *et al*., 2019; Chen *et al*., 2020). While AI-based methods achieve high detection accuracy, their reliance on extensive historical data and cloud computing infrastructure limits practical deployment in low-income regions.

IoT-based smart metering systems have gained traction due to their ability to integrate sensing, communication, and automation (Aswini and Keerthihaa, 2020; Kamatagi *et al*., 2020). However, many implementations focus primarily on billing automation rather than direct physical theft detection.

Recent studies emphasise current-differential techniques as a reliable indicator of bypass events (Yan and Wen, 2021; Calamaro *et al*., 2022). These methods compare meter-side and load-side currents, flagging anomalies when deviations exceed a predefined tolerance. Compared to machine learning methods, threshold-based current differential approaches offer reduced complexity, faster response times, and ease of implementation.

Nevertheless, few studies integrate such techniques with real-time GSM alerts, remote disconnection, and cloud-based visualization in a single low-cost architecture forming the core contribution of this work. This study therefore proposes a current-differential IoT-enabled bypass detection framework tailored for developing-country distribution networks.

MATERIALS AND METHODS USED

The proposed system consists of the following components:

i. Two ACS712 current sensors (meter-side and load-side);

ii. ATmega328p-PU microcontroller for analog-to-digital processing and decision logic;

iii. SIM800A GSM module for SMS alerts;

iv. ESP8266 WiFi module for cloud data transmission;

v. Electromagnetic relay for remote disconnection; and

vi. ThingSpeak® cloud dashboard.

A flow-based algorithm (Fig. 3) monitors current values and triggers detection when the current difference exceeds a tolerance threshold. The proposed system design is organised in the block diagram of Fig. 4.

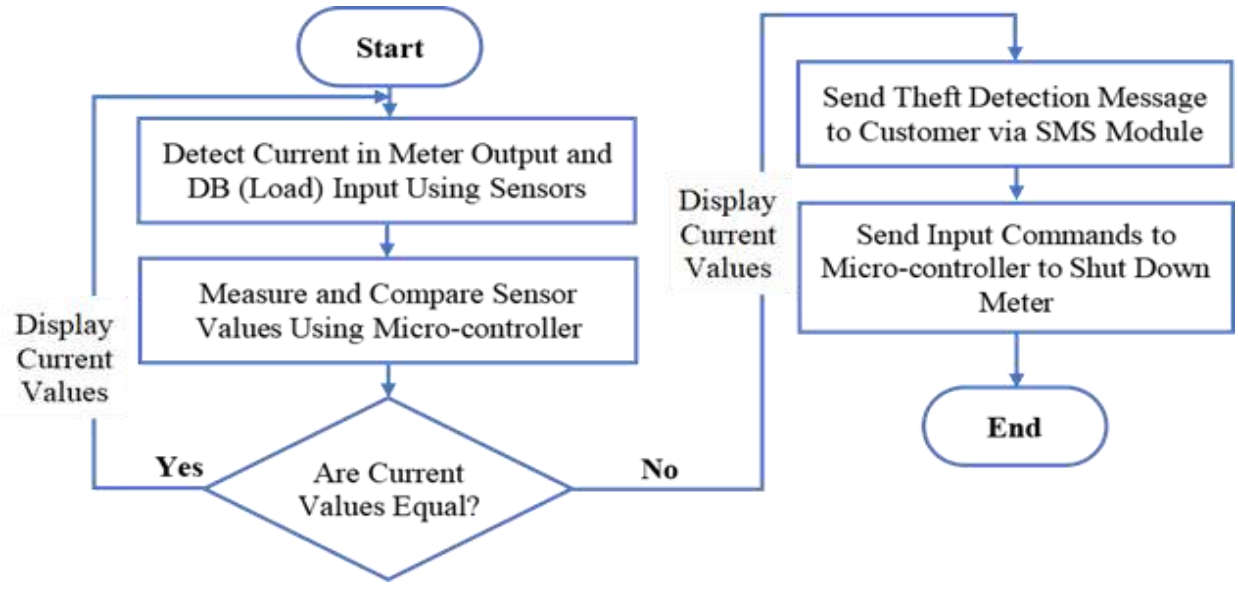

Fig. 3 Flow Chart of Methodology

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XII December 2025

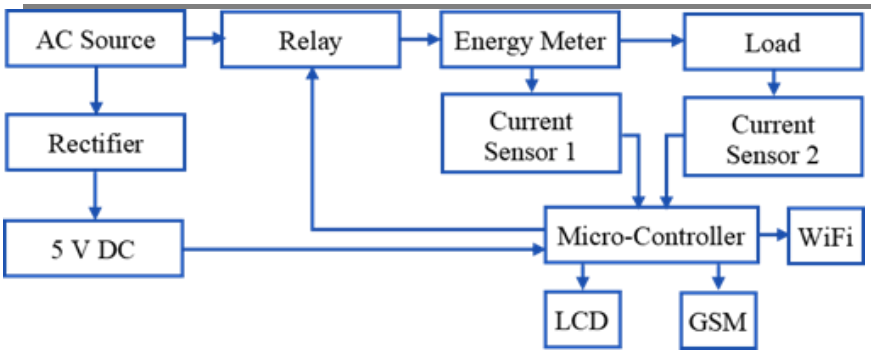

Fig. 4 Block Diagram of Proposed System

Major Components of the System

The system uses an ATmega328p-PU microcontroller, which provides separate memory for instruction handling and data processing, ACS712 Hall-effect current sensors that convert magnetic field variations into proportional voltages for accurate current measurement, and a compact SIM800A GSM module (Fig. 5a) capable of low-power Quad-Band SMS and data transmission to notify customer and utility provider of electricity theft. The ESP8266 (Fig. 5b) is a low-cost, low-power Wi-Fi module with full TCP/IP stack that can operate independently or alongside a microcontroller using standard AT commands, offering flexible programming options. In this design, it connects to the ThingSpeak web platform to upload theft-status data using a generated channel access code, enabling real-time online monitoring. The electromagnetic relay (Fig. 5c) operates through electromagnetic attraction to open or close its contacts, enabling mechanical switching. In this system, the relay disconnects power when the microcontroller issues a shutdown command following theft detection. Its low cost and reliable operation make it an efficient choice for the design. The 16×2 I2C LCD (Fig. 5d) is a compact, easy-to-interface display module capable of showing two lines of text, and in this system it presents theft status and current readings from the meter and load. Its simple wiring, built-in contrast adjustment, and smaller footprint compared to larger LCDs make it a practical and efficient choice for the design.

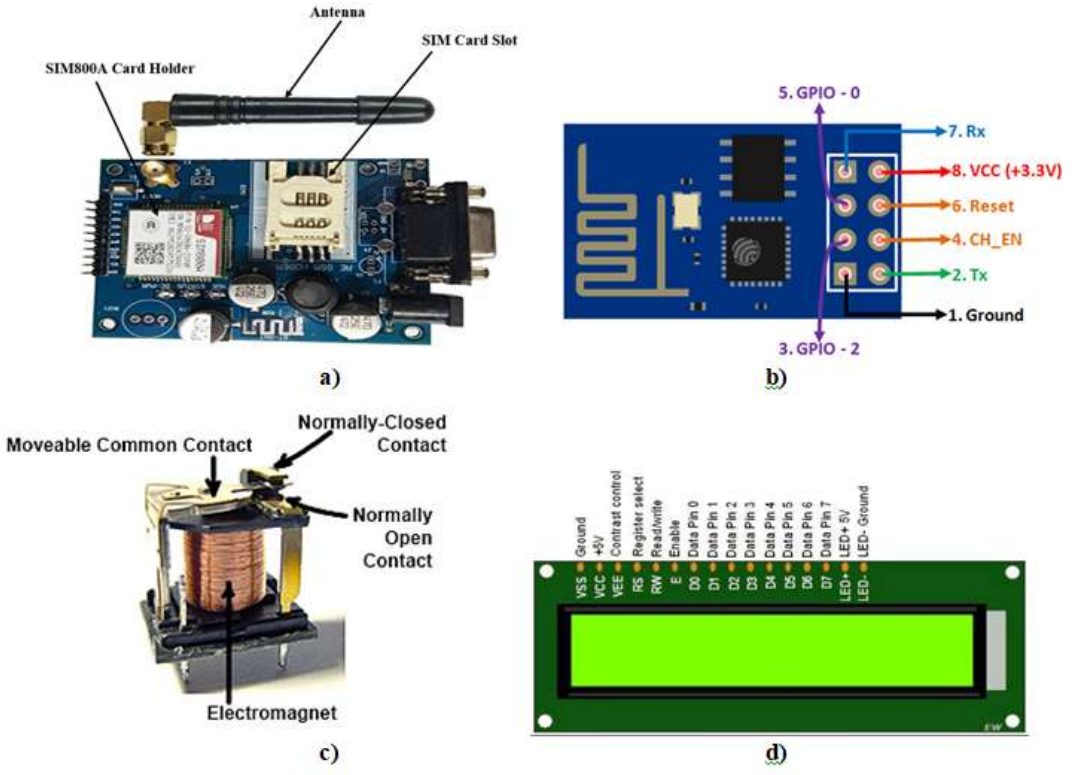

Fig. 5 Main Components of the Proposed System a) SIM800A GSM Module b) ESP8266 WiFi Module c) Electromagnetic Relay and d) 16 × 2 I2C Liquid Crystal Display

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XII December 2025

Mathematical Model for Bypass Detection

The detection model of a smart energy meter compares load-side and meter-side RMS currents using a differential approach (Yan and Wen, 2021), with RMS values obtained using standard Hall-effect measurement techniques (Bansal *et al*., 2022). Because ACS712 sensors exhibit noise and drift, a tolerance of 0.3 A is appropriate for reliable anomaly detection (Datta *et al*., 2019). Threshold-based methods remain widely adopted for tamper and bypass detection (Alfriehat *et al*., 2024). Hence, the change in current, ΔI at the meter side of the smart energy meter, as compared to the load side is given by Equation 1 (Bansal *et al*., 2022).

$$\Delta I = |I_L - I_m| \quad (1)$$

where I_L is the RMS current measured on the load side while I_m is the RMS current measured on the meter side. Using the output voltage V_{pp} of the ACS712 sensor, the RMS voltage V_{rms} could be obtained by Equation 2.

$$V_{rms} = \frac{V_{pp}}{2\sqrt{2}} \quad (2)$$

Adopting sensor sensitivity $S = 100\, mV/A$ and maximum allowable tolerance $T = 0.3\, A$ (Bansal *et al*., 2022), the RMS current I_{rms} could be obtained as given by Equation 3.

$$I_{rms} = \frac{V_{rms}}{S} \quad (3)$$

The bypass detection algorithm of Equation 4 was based on established current-differential threshold methods commonly used in theft detection research (Yan and Wen, 2021; Alfriehat *et al*., 2024; Calamaro *et al*., 2022), where a deviation exceeding a predefined tolerance indicates unauthorised bypassing of the meter as given by Equation 4.

$$If\ \ \Delta I > T \Longrightarrow Bypass\ \ Detected;\ \ Else\ if\ \ \Delta I \leq T \Longrightarrow Normal\ \ Operation \quad (4)$$

Maximum power requirement P_{max} is given by Equation 5.

$$P_{max} = V_{max} \times I_{max} \quad (5)$$

To ensure that the LM7805 does not exceed thermal limits, the regulator power dissipation is carefully analysed based on Equation 6.

$$P_D = (V_{in} - V_{out})\, I_{out} \quad (6)$$

Schematic Diagram of Proposed System

The schematic diagram of the proposed system is shown in Fig. 6, where the AC supply is stepped down and rectified to a regulated 5 V DC, which powers all components of the system. Two ACS712 current sensors measure the meter-side and load-side currents, feeding analogue signals to the microcontroller via pins A0 and A1. The microcontroller computes the RMS values and compares them against a programmed tolerance threshold to determine whether a bypass condition exists. Under normal conditions, the system displays current readings and operational status on the LCD. When the measured difference exceeds the threshold, the microcontroller triggers an alert through the GSM module and awaits a remote shutdown command. Upon receiving this command, it activates the relay (connected to digital pin 19) to disconnect the load. Simultaneously, the ESP8266 WiFi module, interfaced via TX/RX pins, uploads real-time readings and theft-status information to the ThingSpeak platform for cloud monitoring.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XII December 2025

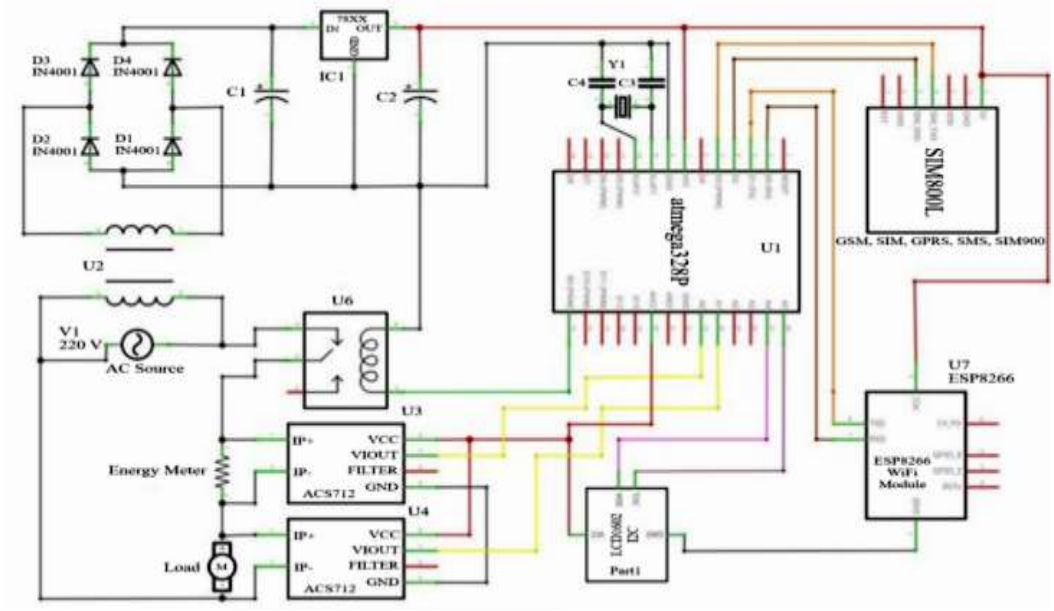

Fig. 6 Circuit Diagram of Proposed System

Proteus Modelling and Simulation

Fig. 7 illustrates the overall architecture of the power-monitoring and bypass-detection subsystem. The AC source provides the primary supply to the system, while relay RL1 serves as the main switching element linking the power source to the rest of the circuitry. RL1 is interfaced with pin 13 of the Arduino Uno microcontroller, enabling the controller to connect or isolate the power path based on the system's decision logic.

Switch S1 routes current through the energy-meter section, represented by resistor R1, thereby simulating normal metering conditions. Conversely, switch S2 introduces a bypass path which diverts current away from the meter, effectively modelling unauthorized meter bypass.

Two current-sensing units form the core of the measurement subsystem. The first sensor, CS1, is positioned in series with the simulated energy meter (R1) to measure the metered current. Its analog output is conditioned by smoothing capacitors C1 and C2, and subsequently fed into the Arduino's A0 analog input pin. The second sensor, CS2, monitors the current supplied to the load. Its output is likewise filtered using capacitors C3 and C4 and routed to analog input A1 of the microcontroller. By comparing the readings from CS1 and CS2, the system could determine whether current bypass occurred.

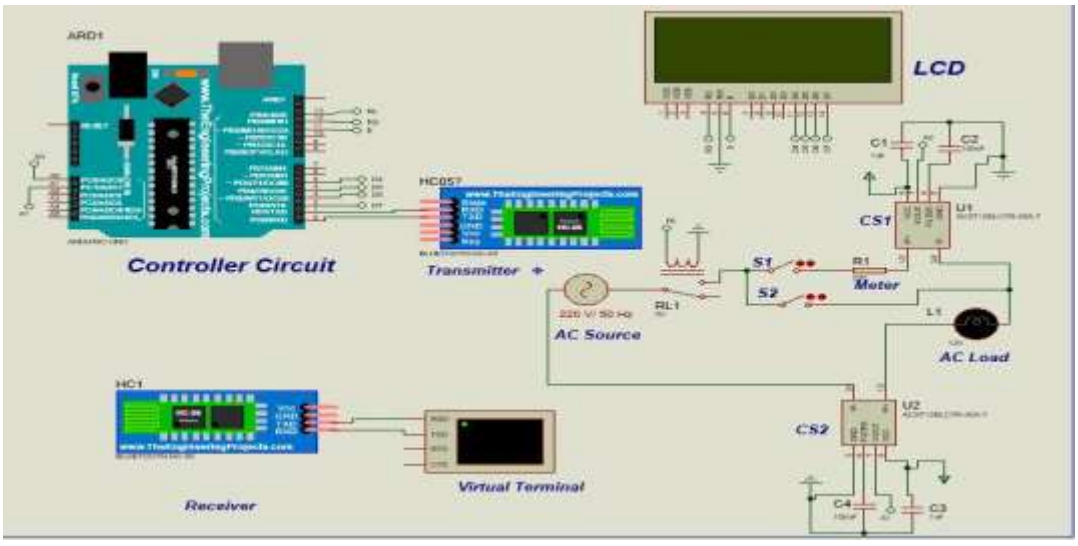

Fig. 7 System Modelling of Design Using Proteus Software

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XII December 2025

Wireless communication is achieved through an integrated Bluetooth module. The transmitter section is connected to the microcontroller's TXD (pin 1) and RXD (pin 0) pins, enabling serial transmission of measurement data to a remote Bluetooth receiver. The receiver's TXD and RXD terminals interface with a virtual terminal, providing real-time visualization of transmitted values during testing and debugging. Additionally, a 16 × 2 LCD module is connected to the microcontroller via pins RS, E, D4, D5, D6, and D7, serving as a local display interface for system status and real-time sensor outputs.

System Implementation and Testing

The implemented IoT-based electricity-theft monitoring system is presented in Figure 8. The prototype comprises an energy meter, two ACS712 current sensors, a relay unit, a 16 × 2 I²C LCD, an Atmega328P-PU microcontroller, a power supply module, a bulb acting as the controlled load, and a breadboard for component interconnections.

The power-supply module delivers regulated DC power to the microcontroller, sensors, communication modules, and peripheral components. The two ACS712 current sensors independently measure the current flowing through the meter and the current supplied directly to the load. These measurements are continuously sampled by the Atmega328P-PU microcontroller, which executes the decision logic required to classify system states as either "theft" or "no-theft."

When a discrepancy indicative of bypass is detected, the microcontroller triggers a series of automated responses:

i. The relay unit, also powered by the supply module, is energized to open the power circuit, thereby disconnecting supply to the load;

ii. The SIM800A GSM module then transmits an SMS alert to the designated utility authority, notifying them of the detected tampering event; and

iii. The ESP8266 Wi-Fi module uploads real-time current readings and system status to the ThingSpeak® cloud platform, enabling remote monitoring and long-term data analytics.

During normal operation, all real-time current measurements and system states are displayed on the 16 × 2 I²C LCD, offering instantaneous local feedback.

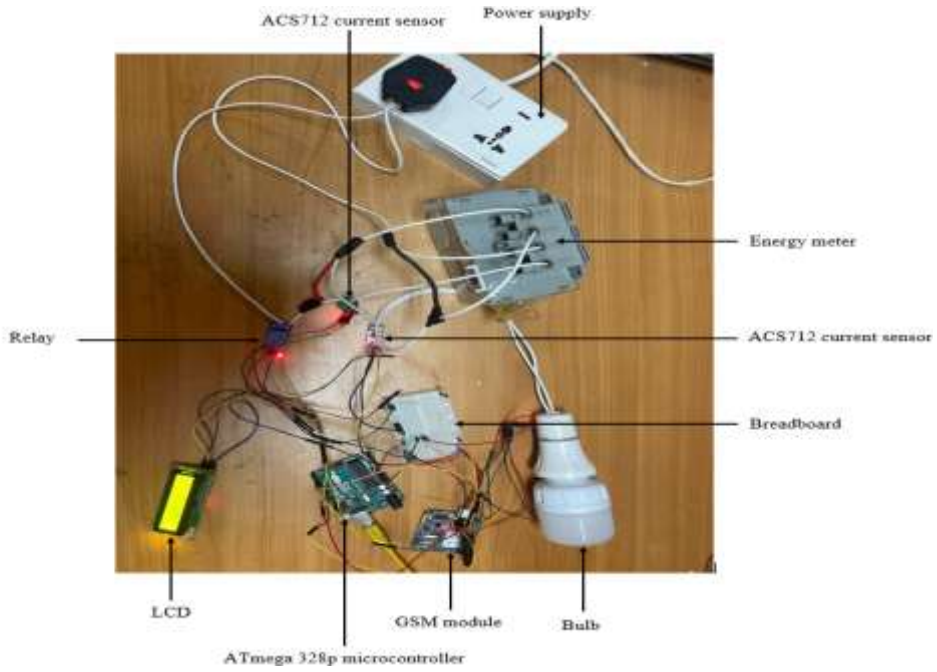

Fig. 8 Prototype of Proposed Design

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XII December 2025

RESULTS AND DISCUSSION

Initial Operating Condition

Under idle conditions, no current flows through either the energy meter sensing path or the load sensing path because relay RL1 is open and both switches S1 and S2 are inactive. Both current sensors, CS1 and CS2, register zero current, yielding,

$$\Delta I = | I_L - I_m | = | 0 - 0 | = 0\ A \qquad (7)$$

which is below the detection threshold. The system correctly classifies this as a non-theft state. The LCD displays the name of the system as "Theft Detection System" as shown in Fig. 9.

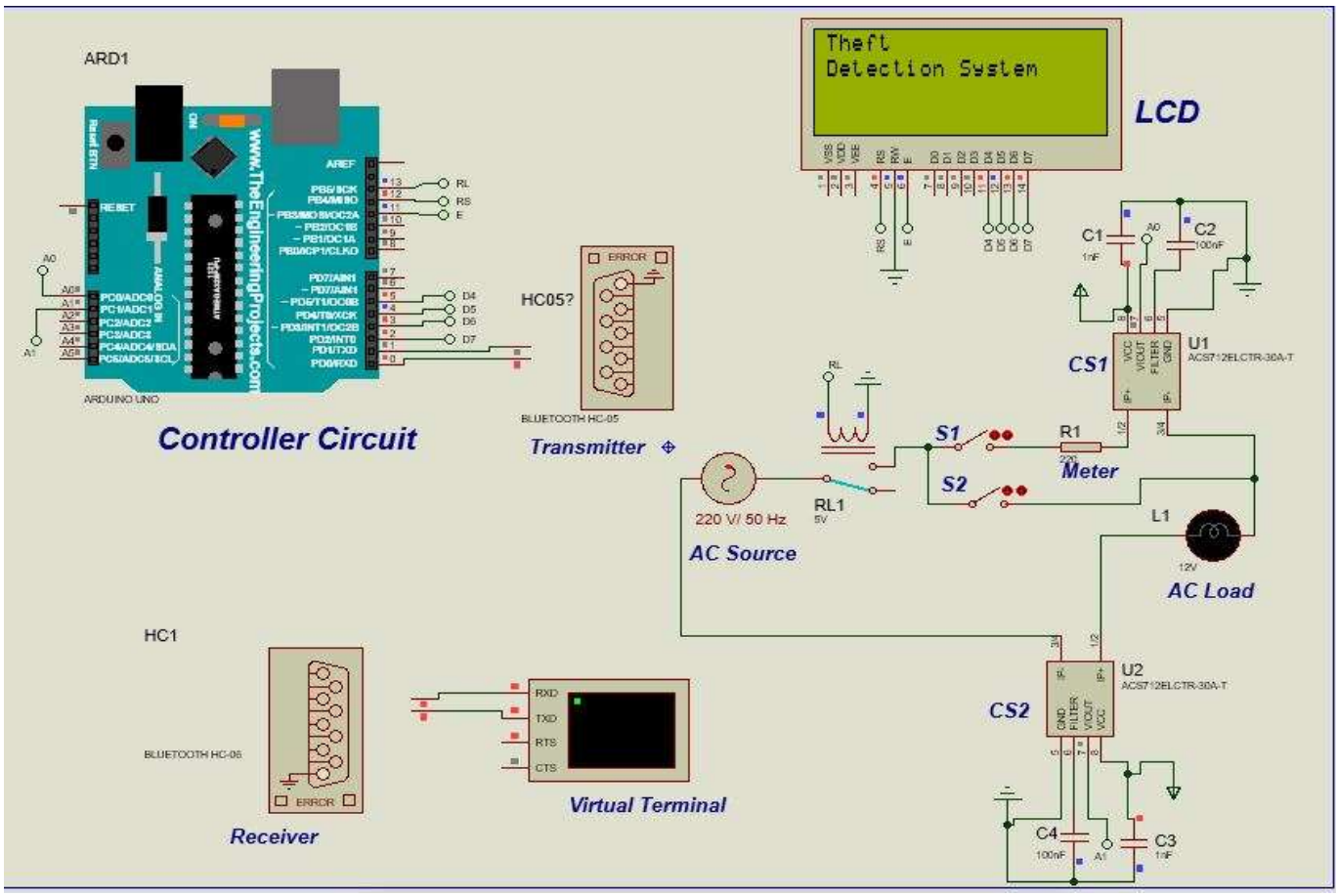

Fig. 9 Initial State of Operation

Normal Metered Operation

During normal operation when RL1 energizes and switch S1 is closed, current flow through both the energy meter and the load. Typical measured values of

$$I_m = 0.50\ A \quad and \quad I_L = 0.49\ A \qquad (8)$$

produce a differential of $\Delta I = 0.01$ A confirming legitimate consumption. Consequently, the system interprets this as a non-theft condition and the LCD simultaneously displays both current readings together with the message "No Theft Detected" (Fig. 10) since the change in current falls within the acceptable measurement tolerance.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XII December 2025

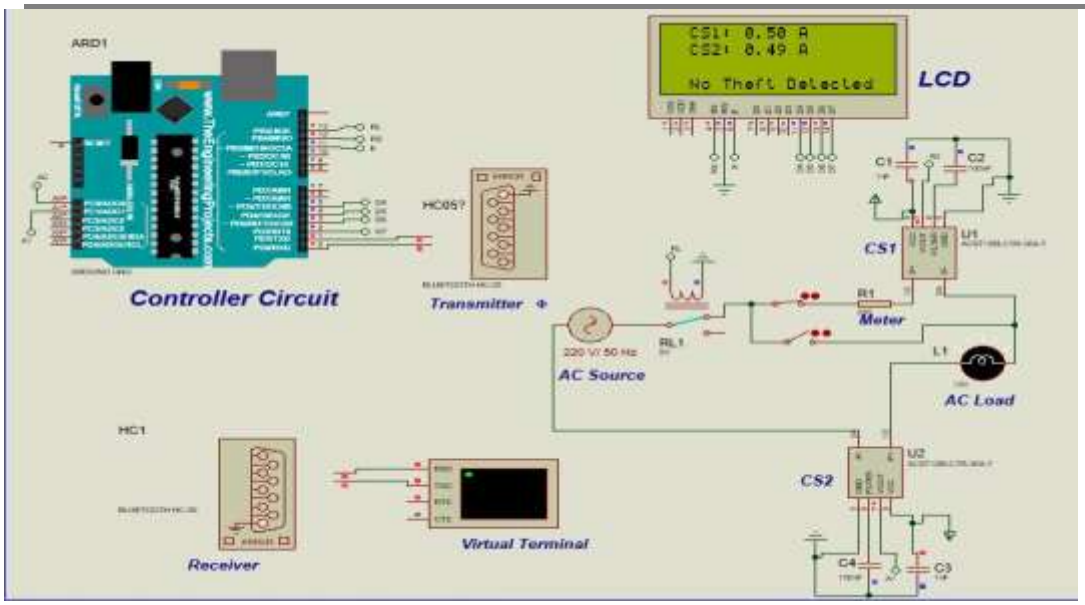

Fig. 10 Result of Simulation when Power Passes through the Energy Meter

Meter Bypass Condition and Operability

When bypass is introduced, the meter-side current drops to zero while load current persists. This results in $\Delta I = | 0.50 - 0.00 | = 0.50\ A$ exceeding the threshold. The system immediately flags theft (Fig. 11), sends SMS alerts, uploads status to ThingSpeak®, and disconnects the load via relay control. Cloud-based current-time plots clearly show divergence between meter and load currents, followed by system shutdown, validating the effectiveness of the detection algorithm.

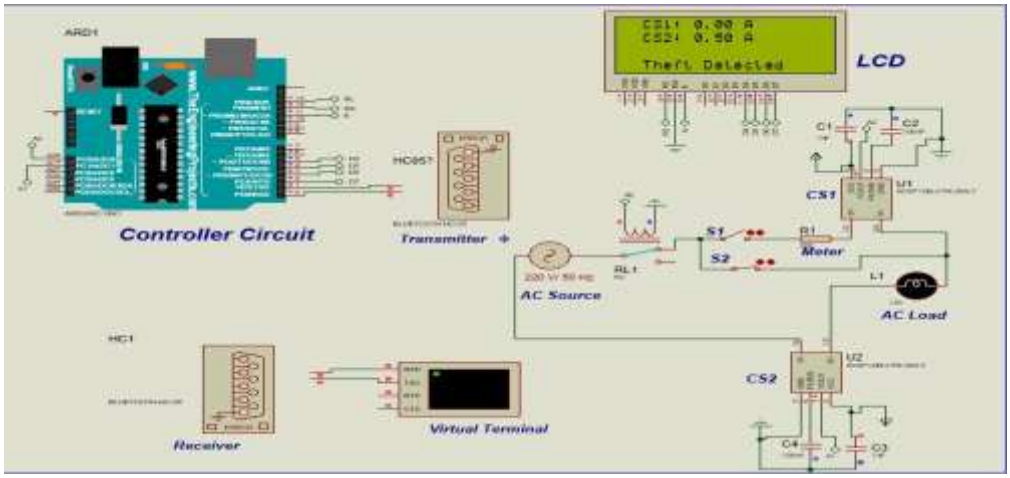

Fig. 11 Results of Simulation when Power Bypasses the Meter

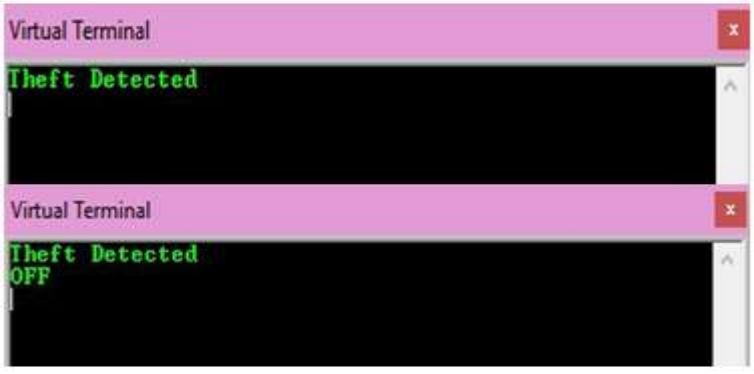

Fig. 12 Virtual Terminal Interface Showing Notification of Theft

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XII December 2025

Theft detected is displayed on a virtual terminal of the receiver Bluetooth component as shown in Fig. 12a. The receiver sends an "OFF" command which is indicated in Fig. 12b to shut down the system (Fig. 13). This command is sent via wireless means from the receiver Bluetooth to the transmitter Bluetooth and then to the microcontroller. However, the Bluetooth communication is used primarily in the Proteus simulation for shutdown testing, as a development abstraction and commissioning mode scenarios. For deployment purposes, the GSM and Wi-Fi modules are employed. Wi-Fi cloud reporting could also be employed where the ESP8266, which natively supports TLS-encrypted HTTPS communication, is enabled when transmitting data to ThingSpeak® to prevent packet sniffing or man-in-the-middle attacks. Device authentication using API keys bound to unique meter IDs may also be integrated to ensure traceability and prevent unauthorized data injection into utility dashboards (Al-Fuqaha *et al*., 2015).

To unify GSM and Wi-Fi modules, a single command-handling state machine is proposed where all shutdown commands, whether originating from SMS, cloud dashboards, or future utility SCADA integration, should be routed through a common command parser with identical authentication checks. Bluetooth control may be retained exclusively for laboratory diagnostics, gated behind a hardware jumper or firmware compile flag. In operational mode, only GSM-authenticated commands would be accepted, ensuring consistent behaviour across simulation and deployment. The unified logic improves maintainability, reduces firmware branching errors, and aligns with best practices in cyber-physical system design (Cárdenas *et al*., 2008).

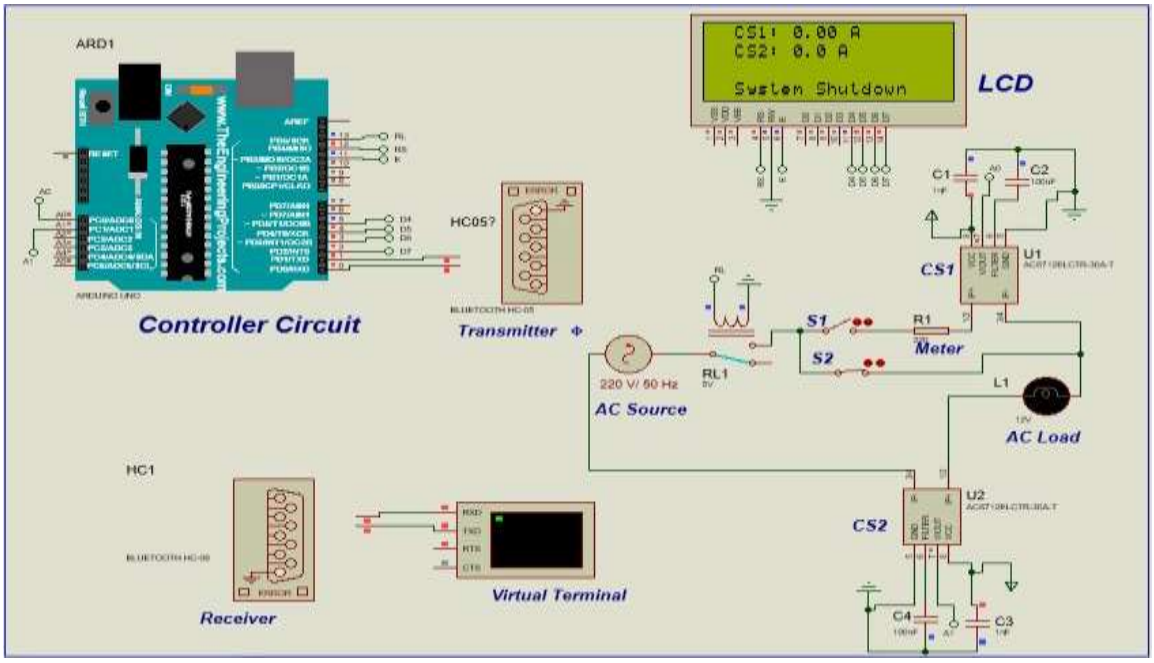

Fig. 13 System Shut Down Simulation Results

SMS and Cloud Reporting Reliability

The dual-channel reporting strategy (SMS + cloud) significantly enhances system resilience. SMS alerts provide low-latency, point-to-point notification, particularly valuable in rural or bandwidth-limited regions. Cloud reporting, conversely, enables long-term analytics, trend identification, and regulatory auditing (Gungor *et al.*, 2013). To improve reliability under unstable network conditions, a store-and-forward data mechanism is recommended. Theft events, timestamps, and current values should be cached locally in non-volatile memory (EEPROM or external FRAM). When connectivity is unavailable, events are logged locally; once GSM or Wi-Fi connectivity is restored, buffered records are automatically uploaded to the cloud. This approach ensures zero data loss, supports forensic investigations, and aligns with fault-tolerant IoT design principles (Zanella *et al*., 2014).

Cost–Benefit and Return-on-Investment (ROI) Analysis

The bill of materials for components used for system implementation of Figs. 6 and 8 are given in Table 1.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XII December 2025

Table 1 Bill of Materials for Components Used for System Implementation

SN	Item	Quantity (pcs)	Unit Cost (GH¢)	Total Cost (GH¢)	Store
1.	Rectifier Diodes 1N4007	4	1.00	4.00	GeekElectronics
2.	Step Down Transformer (240/9 V, 1 A)	1	70.00	70.00	AnyComponentLab
3.	Capacitors (470 µf)	1	1.20	1.20	Oku Electronics
4.	Capacitors (100 µf)	1	0.80	0.80	Oku Electronics
5.	LM7805 IC Voltage Regulator	1	6.50	6.50	Nauvitel
6.	Printed Circuit Board (small, custom)	1	15.00	15.00	AnyComponentLab
7.	Atmega 328p-pu microcontroller (DIP)	1	74.00	74.00	Nauvitel
8.	ACS712 Allegro Current Sensors	2	30.00	60.00	AnyComponentLab
9.	SIM800A GSM Module	1	80.00	80.00	DaakyeTech
10.	ESP8266 WiFi Module	1	20.00	20.00	DaakyeTech
11.	Electromagnetic Relay 10A 5V	1	11.00	11.00	Nauvitel
12.	16 × 2 I2C Liquid Crystal Display	1	40.00	40.00	DaakyeTech
13.	Enclosure, terminals, wiring, fusing/TVS protection, PCB finishing, assembly/testing, SIM, logistics.		150.00	150.00	
Total				**532.50**	

A preliminary economic analysis demonstrates strong financial justification for deployment. The estimated unit cost of the proposed system, including sensors, microcontroller, GSM module, Wi-Fi module, relay, and enclosure was Gh¢ 532.50 (Table 1) which was equivalent to US$ 46.91 as of 4th December 2025 according to the daily interbank FX Rates of the Bank of Ghana where Gh¢ 1.00 was equivalent to US$ 0.0881.

For a typical low income consumer having an annual bill B of Gh¢ 4000.00 /year and considering a system loss reduction of 30%, recovered revenue/year will be equivalent to 0.1286×4000 = Gh¢ 514.40/year of which the payback, which is a fraction of the deployed unit cost to the recovered revenue/year, would be approximately 532.50/463 which results in payback within the first year, with continued revenue recovery thereafter (Equations 9 to 12).

$$Delivered\ value = \frac{B}{0.7} \quad (9)$$

$$Loss\ value = Delivered - B = \frac{B}{0.7} - B = 0.4286 \times B \quad (10)$$

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XII December 2025

Applying "30% loss reduction", recovered revenue per year:

$$Recovered = 0.30 \times Loss\ value = 0.1286 \times B = 12.9\%\ of\ annual\ billed\ revenue, B \quad (11)$$

$$Payback = \frac{Deployed\ unit\ cost}{Recovered\ revenue/year} \quad (12)$$

A preliminary economic analysis demonstrates strong financial justification for deployment. This favourable Retun On Investment (ROI), combined with minimal infrastructure modification and retrofit compatibility, makes the proposed system economically attractive for utilities in developing economies (Yakubu *et al*., 2018; Yan and Wen, 2021).

CONCLUSIONS

The study successfully demonstrates an IoT-enabled, current-differential electricity theft detection system capable of identifying meter bypass events in real time. The proposed design integrates sensing, analytics, communication, and control into a compact solution. Experimental results confirm reliable detection, remote alerting, automated disconnection, and cloud-based monitoring.

RECOMMENDATIONS

Based on the results obtained in this research, it is recommended that:

i. Utility companies could consider deployment of the current-differential IoT monitoring unit as a retrofit solution for legacy meters;

ii. Threshold calibration could be adapted based on network characteristics and sensor accuracy; and

iii. Integration with utility billing and outage management systems could enhance operational efficiency.

The following reasoning and recommendation could also be considered.

Security of Communication Links and Data Integrity

While the proposed system effectively demonstrates current-differential detection and remote intervention, the security of its communication pathways is critical for real-world deployment. The architecture employs GSM (SIM800A) for SMS alerts, ESP8266 Wi-Fi for cloud reporting, and short-range Bluetooth communication during simulation and testing. Each interface introduces distinct security risks that must be mitigated to prevent spoofing, false shutdown commands, or data manipulation. SMS communication over GSM networks is inherently vulnerable to SIM cloning, SMS spoofing, and replay attacks, particularly in regions with weak telecom authentication infrastructure (Deva and Akashe, 2017).

To address the SMS/GSM vulnerability issues, command authentication should be implemented using message hashing with shared secrets, where shutdown commands include a hashed token derived from a time-varying nonce and a pre-shared key stored in the microcontroller's EEPROM. Lightweight cryptographic schemes such as HMAC-SHA1 or AES-128 in CBC mode are computationally feasible on ATmega328P-class microcontrollers and significantly improve command authenticity (Perrig *et al*., 2004; Roman *et al*., 2018).

Long-Term Hardware Stability in Poor-Quality Grids

Low-voltage distribution networks in developing regions are frequently subject to voltage sags, surges, switching transients, and lightning-induced spikes. These disturbances pose a significant threat to microcontroller-based monitoring devices. Long-term stability analysis indicates that without protection, components such as the ACS712 sensors, ATmega328P, SIM800A, and ESP8266 are vulnerable to cumulative dielectric stress and latch-up failures (IEEE Std 1159-2019).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XII December 2025

To enhance durability, it is recommended that Metal Oxide Varistors (MOVs) and Transient Voltage Suppression (TVS) diodes be integrated at the AC input. Additionally, an RC snubber networks across relay contacts could be implemented to suppress inductive kickback while alternative isolated DC-DC converters for communication modules could be installed to prevent conducted EMI coupling. These protection schemes would enable the system to achieve multi-year operational stability comparable to commercial smart meters deployed in harsh grid environments (Sadeghi *et al*., 2017).

Multi-Parameter Detection to Reduce False Positives

While current-differential analysis is highly effective for bypass detection, it may misclassify certain legitimate events such as motor inrush currents or voltage collapse under heavy load. To improve discrimination, voltage magnitude and power factor monitoring can be incorporated. A genuine load anomaly typically exhibits simultaneous current increase, voltage drop, and power-factor deviation, whereas meter bypass results in current mismatch without corresponding voltage-PF behaviour. By implementing a multi-parameter decision rule as given by Equation 13,

$$Theft = (\Delta I > \delta_I) \wedge (|\ \Delta V\ | < \delta_V) \wedge (|\ \Delta cos\phi\ | < \delta_\phi) \quad (13)$$

false positives could be significantly reduced thereby improving utility confidence and customer acceptance (Depuru *et al*., 2011; Calamaro *et al*., 2022).

Future works should consider the following:

i. Perform iterations to address cybersecurity by incorporating basic encryption for the ESP8266 and SIM800A transmissions to prevent data tampering; and

ii. Conduct field trials in varying environmental conditions to help refine "tolerance threshold (T)" for more diverse network characteristics.

REFERENCES

1. Alfriehat, N., Anbar, M., Aladaileh, M., Hasbullah, I., Shurbaji, T.A., Karuppayah, S. and Almomani, A. (2024), RPL-Based Attack Detection Approaches in IoT Networks: Review and Taxonomy, Artificial Intelligence Review, 57(9), p.248.
2. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M. (2015), "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications", IEEE Communications Surveys & Tutorials, 17(4), pp. 2347–2376.
3. Aswini, R., and Keerthihaa, V. (2020), "IoT Based Smart Energy Theft Detection and Monitoring System for Smart Home", International Conference on System, Computation, Automation and Networking (ICSCAN), Puducherry, India pp. 1 – 6.
4. Bansal, D., Gupta, K., Sharen Ganesh, M.C., Goyal, J., Tharani, K. and Sharma, S. (2022), "Smart Energy Meter Based on Hall Effect Current Sensing Techniques with IoT Modules". Journal of Information and Optimization Sciences, 43(1), pp.225-231.
5. Calamaro, N., Levy, M., Ben-Melech, R. and Shmilovitz, D., 2022. TNT Loss: A Technical and Nontechnical Generative Cooperative Energy Loss Detection System. Sensors, 22(18), p.7003.
6. Cardenas, A. A., Amin, S. and Sastry, S. (2008), "Secure Control: Towards Survivable Cyber-Physical Systems", 28th International Conference on Distributed Computing Systems Workshops, pp. 495-500.
7. Chen, Y., Hua, G., Feng, D., Zang, H., Wei, Z., and Sun, G. (2020), "Electricity Theft Detection Model for Smart Meter Based on Residual Neural Network", 12th IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), Xi'an, China, pp. 1 – 5.
8. Czechowski, R., and Kosek, A. M. (2016), "The Most Frequent Energy Theft Techniques and Hazards in Present Power Energy Consumption", IEEE Proceedings of the 2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG), Vienna, Austria, pp. 1 – 7.

9. Datta, A., Raj, K. and Sarker, R., 2019, September. Implementation of a high accuracy ac current sensing scheme using hall-sensor. In 2019 International Conference on Energy Management for Green Environment (UEMGREEN) (pp. 1-4). IEEE.
10. De Souza, M. A., Pereira, J. L., Alves, G. D. O., de Oliveira, B. C., Melo, I. D., and Garcia, P. A. (2020), "Detection and Identification of Energy Theft in Advanced Metering Infrastructures", Electric Power Systems Research, Vol. 182, p. 106258.
11. Depuru, S. S. S. R., Wang, L. and Devabhaktuni, V. (2011), "Electricity Theft: Overview, Issues, Prevention and a Smart Meter Based Approach", Energy Policy, 39(2), pp. 1007–1015.
12. Deva, S.V.S.V.P. and Akashe, S. (2017), "Implementation of GSM Based Security System with IOT Applications". International Journal of Computer Network and Information Security, 14(6), 13 p..
13. Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C. and Hancke, G. P. (2013), "Smart Grid Technologies: Communication Technologies and Standards", IEEE Transactions on Industrial Informatics, 7(4), pp. 529–539.
14. Kamatagi, A. P., Umadi, R. B., and Sujit, V. (2020), "Development of Energy Meter Monitoring System (EMMS) for Data Acquisition and Tampering Detection using IoT", Proceedings of CONECCT 2020 - 6th IEEE International Conference on Electronics, Computing and Communication Technologies, Bangalore, India, pp. 1 – 6.
15. Perrig, A., Stankovic, J. and Wagner, D. (2004), "Security in Wireless Sensor Networks", Communications of the ACM, 47(6), pp. 53–57.
16. Roman, R., Lopez, J. and Mambo, M. (2018), "Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges", Future Generation Computer Systems, 78, pp. 680–698.
17. Sadeghi, A. R., Wachsmann, C. and Waidner, M. (2017), "Security and Privacy Challenges in Industrial Internet of Things", Proceedings of the 52nd Annual Design Automation Conference, pp. 1–6.
18. Tangsunantham, N., Suchat, N., Varunyou N., Somchai T., and Chaiyod P. (2013), "Experimental Performance Analysis of Current Bypass Anti-Tampering in Smart Energy Meters", Australasian Telecommunication Networks and Applications Conference (ATNAC), Christchurch, New Zealand, pp. 124 – 129.
19. Yakubu, O., Babu, N. and Adjei, O. (2018), "Electricity theft: Analysis of the underlying contributory factors in Ghana", Energy Policy, Vol. 123, pp. 611 – 618.
20. Yan, Z. and Wen, H. (2021), Performance Analysis of Electricity Theft Detection for the Smart Grid: An Overview. IEEE Transactions on Instrumentation and Measurement, 71, pp.1-28.
21. Yao, D., Wen, M., Liang, X., Fu, Z., Zhang, K., and Yang, B. (2019), "Energy Theft Detection with Energy Privacy Preservation in the Smart Grid", IEEE Internet of Things Journal, Vol. 5, No. 6, pp. 7659 – 7669.
22. Zanella, A., Bui, N., Castellani, A., Vangelista, L. and Zorzi, M. (2014), "Internet of Things for Smart Cities". IEEE Internet of Things journal, 1(1), pp.22-32.

Dr John Kojo Annan presently lectures at the Department of Electrical and Electronic Engineering of the University of Mines and Technology (UMaT), Tarkwa, Ghana. He holds PhD and MPhil degrees in Electrical and Electronic Engineering from UMaT. He also holds a BSc degree in Electrical and Electronic Engineering from the Kwame Nkrumah University of Science and Technology (KNUST), Kumasi. He is a member of the Institute of Electrical and Electronics Engineers, International Association of Engineers, and Society of Petroleum Engineers. His research interests are in Power Systems, Renewable Energy Systems, Computer Applications, Control Systems, and Electrical Applications in Biomedical Systems.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XII December 2025

Lordina Eshun is currently an M.S. student in Electrical and Computer Engineering at the University of Memphis, United States. She holds a BSc degree in Electrical and Electronic Engineering from the University of Mines and Technology (UMaT), Tarkwa, Ghana. She has four years of professional experience in the mining industry, with specialization in electrical systems, reliability engineering, and maintenance optimization. Her work focused on improving equipment uptime, asset availability, and energy efficiency across large-scale industrial systems. Her research and professional interests include energy optimization, robotics, artificial intelligence, automation, and control systems.