

Energy Theft Detection and Real-Time Monitoring in a Smart Prepaid Metering System

Qudus Omotayo Ajiboye¹, Tosin Gideon Olaleye², Agada Olowu Innocent³,
Yusuff Afees Ademola⁴, Victor Ikechukwu Stephen⁵, Abimbola Olamide⁶,
Abiodun Taiwo⁶, Moses Sodiq Sobajo⁷

¹ *Yaba College of Technology*

Herbert Macaulay Road, Opposite WAEC office, Yaba, Lagos State, Nigeria

² *The Federal Polytechnic, Ado-Ekiti*

P. M. B. 5351, Ado-Ekiti, Ekiti State, Nigeria

³ *Ahmadu Bello University*

Samaru Campus, Community Market, Zaria, 810211, Kaduna, Nigeria

⁴ *Ladoke Akintola University of Technology*

Old, Oyo/ Ilorin Rd, Ogbomosho 210214, Nigeria

⁵ *Michael Okpara University of Agriculture*

P. M. B. 7267 Umuahia Umudike, Abia State, Nigeria

⁶ *North Carolina Agricultural and Technical State University*

1601, E. Market Street, Greensboro, NC, 27411, USA

⁷ *De Montfort University*

The Gateway House, Leicester, Leicestershire, LE1 9BH, United Kingdom

DOI: [10.22178/pos.107-19](https://doi.org/10.22178/pos.107-19)

LCC Subject Category: T1-995

Received 25.06.2024

Accepted 28.08.2024

Published online 31.08.2024

Corresponding Author:

Qudus Omotayo Ajiboye

qudusboye@gmail.com

© 2024 The Authors. This article is licensed under a [Creative Commons Attribution 4.0](https://creativecommons.org/licenses/by/4.0/)

License 

Abstract Electricity theft represents a significant financial loss for distribution companies, primarily caused by consumer activities such as energy meter bypassing and tampering. This research presents a study approach to an intelligent prepaid energy metering system designed to detect and address these issues while offering real-time monitoring capabilities. The system is built around a microcontroller which monitors readings from two current sensors, one tracking the user's load consumption and being placed before the meter to measure the total current drawn by all the loads. Any changes between these readings indicate theft, prompting immediate action. A momentary switch is installed to detect tampering attempts and automatically trigger alerts once the meter is tampered with. Also, the system enables users to recharge energy units remotely and monitor their consumption through a user-friendly interface. The inclusion of GSM technology ensures that all unauthorized activities are reported to the relevant authorities. Experimental results demonstrate that the system measures load consumption and detects attempts to bypass the meter, reducing utility companies' revenue losses.

Keywords: Electricity; Monitoring; Real-time.

INTRODUCTION

Electricity theft is a significant challenge for power systems worldwide, with no system immune to such losses. 1999 Transparency International reported that nearly 15% of the

generated electricity is lost because of theft. For example, between 1998 and 1999, the Bangladesh Power Development Board (BPDB) produced approximately 14,600 MWh of electricity in Bangladesh. Still, it could only account for 11,462 MWh of billed energy, resulting in a total loss of

about 22% [1]. In developing countries like Nigeria, electricity theft continues to be one of the major obstacles for the power sector because the government lacks controls to advanced technology for effective prevention. The adoption of Automatic Metering Infrastructure (AMI) has reduced the need for manual meter readings but has also led to increased non-technical losses for utility companies [2].

It is calculated that Nigeria's electrical grid experiences transmission and distribution (T&D) losses of around 40%, which is significantly higher compared to the United States, where T&D losses are approximately 7% [3, 4]. Electricity theft is any partial or complete interference bypassing meter readings to reduce energy charges [5]. Human activities, including meter tampering, bypassing, billing irregularities, and unpaid bills, cause non-technical losses. Dealing with this rising problem calls for quick actions to improve the capacity for power generation and the efficiency and smartness of energy consumption, especially in the home sector.

Still common in many areas of Nigeria, analogue meters provide significant difficulties in precisely tracking energy consumption. Power Utility technicians must personally visit a consumer's house with these meters to terminate the electricity supply for non-payment. This process is sometimes undermined by consumer bribery and meter tampering. Moreover, analogue meters do not allow consumers to remotely disconnect their power when away from home, leading to unnecessary energy consumption and increased costs. While prepaid meters have improved the monitoring of power usage, the issue of electricity theft through meter bypassing and tampering remains a critical concern.

Electricity Theft and Its Impact. Electricity theft is a significant contributor to non-technical losses. In addition, end-user bypassing tactics allow tampering with the meter to defraud the utility providers [5]. Energy theft occurs among two groups: non-consumers and legitimate consumers. The following actions by consumers are commonly associated with electricity theft [5]:

Methods of Electricity Theft:

1. **Tampering with the Energy Meter:** Consumers may physically alter the meter to record lower consumption.

2. **Bypassing the Electric Meter:** Some consumers connect directly to the power source, bypassing the meter entirely.

3. **Evading Payment:** This includes non-payment of bills and billing irregularities.

4. **Using Magnets and Reversing Current:** In analogue disc-type energy meters, consumers might use magnets or reverse current direction by changing the terminals to manipulate readings.

5. **Radio Frequency Devices:** These devices are employed to tamper with electronic meters.

6. **Intermittent and Opportunistic Theft:** Even well-off consumers may occasionally commit theft when the opportunity arises.

7. **Illegal Neutral Disconnection:** Some illegal customers disconnect the neutral wire from the return path, causing the energy meter to assume that the voltage between the live wire and the new neutral is zero, which results in the meter reading zero energy consumption.

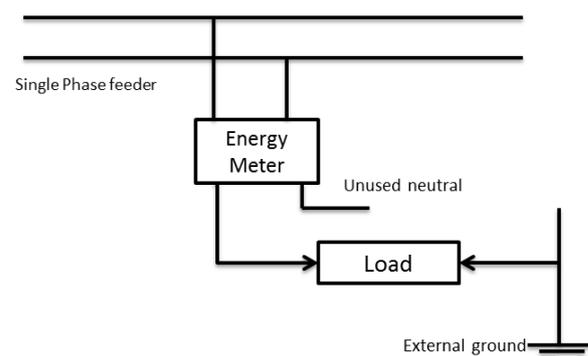


Figure 1 – Illustration of Neutral Disconnect Method for Electricity Theft

8. **Current Transformer (CT) Tampering:** Insulating or damaging a current transformer's secondary terminal or control wires can reduce the measured current, leading to inaccurate energy readings.

9. **Analyzing Power System Losses:** A thorough analysis of power system transmission and distribution (T&D) losses can provide accurate theft estimates. Implementing substantial technical improvements, along with intelligent and proactive anti-theft measures, can significantly improve the performance of power utilities.

While technical solutions like tamper-proof meters, anti-theft cables, prepayment meters, GSM-based technologies, and managerial methods such as inspection, monitoring, and restructuring distribution systems can reduce electricity theft, it remains a persistent issue. The distribution system must be sufficiently intelligent to accurately identify and localize the degree and location of theft to create accountability and effectively combat this challenge [2, 6, 7, 8].

Review of related works

Preventing Theft in Smart Electrical Distribution Systems through Advanced Metering [9, 10]. An approach to combat energy theft within intelligent electrical distribution systems was proposed, focusing on pinpointing the location and extent of electricity theft using Power Line Communication (PLC) as part of Automatic Metering Infrastructure (AMI). The method utilizes the inherent signal degradation during analogue signal transmission over power lines. By monitoring the signal's deterioration, the system can diagnose and locate instances of theft. PLC modulates a carrier frequency on the existing power line, enabling meters to communicate with each other. When meter A sends a signal to meter B, and no theft has occurred, meter B acknowledges and relays the signal back to the base station without any degradation.

Conversely, if theft occurs, the signal deteriorates, and meter B reports this discrepancy to the central station. The level of signal degradation corresponds to the amount of electricity stolen, allowing the system to estimate the extent of theft. To function effectively, all meters in this system must be equipped with PLC handshaking capabilities and filters to ensure accurate signal comparison.

Intelligent Metering System for Controlling and Preventing Electricity Theft. Nabil Mohammed et al. developed a prepaid energy metering system to control electricity theft [11–13]. This system includes a single-phase smart meter installed at the consumer's premises, which communicates with a server operated by the utility company using GSM modules for bidirectional communication. The system's core components are an ATmega 32 microcontroller, an ADE7751 energy measurement chip, a Siemens A62 mobile phone as the GSM module, MAX232, current and

potential transformers, an LCD, and a relay. The microcontroller calculates energy consumption based on pulses generated by the energy metering chip. The meter has two current transformers that monitor current flow in the phase and neutral lines to detect theft, mainly through phase and neutral line short-circuiting. If the current values differ significantly, the microcontroller triggers a relay to disconnect the power supply and sends an alert to the server, indicating possible theft. Additionally, lever switches are installed to detect meter tampering, sending an alert to the server if tampering is detected.

Automated Metering Interface for Theft Prevention. Authors [10, 14] introduced an anti-theft automatic metering interface using an Arduino microcontroller to continuously monitor and store energy meter readings. A GSM module enables remote monitoring and control, while a comparator circuit detects meter bypassing. The comparator compares input values before and after the meter, feeding any discrepancies to the microcontroller, which indicates bypassing. A tactile sensor detects meter tampering by sensing touch, force, or pressure changes. This system relies on the GSM network to communicate instances of theft to the utility provider.

Electricity Theft Detection System Utilizing Advanced RISC Machine (ARM) Processor and GSM Network. A system utilizing an LPC1343 ARM processor was developed to control electricity theft. This system is similar to the one Nabil Mohammed et al. proposed but introduces a four-terminal output-regulated potential transformer [15–18]. One terminal connects directly to the energy measuring unit, while the remaining terminals regulate the power supply to the ARM processor and GSM module. This configuration reduces costs and enhances efficiency. The system can detect various theft modes by simulating phase and neutral line shorts, with alerts sent via SMS using the GSM network. The system's low power consumption makes it a cost-effective solution for energy theft detection.

Advanced Theft Detection System for Prepaid Energy Meters in Nigeria. The advanced theft detection system for prepaid energy meters was introduced to identify and eradicate electricity theft [15, 17]. The proposed power theft detection system is made up of three components:

1. Intelligent Prepaid Meter (IPEM): This is installed at the consumer's end. It is designed to monitor and record energy consumption in real-

time. It has advanced sensors and processing capabilities to detect bypasses and alterations in energy usage patterns that may indicate theft.

2. Intelligent Power Theft Detection System (IPTDS): This is located at the transformer or electric pole. It monitors the power flowing through the distribution network. It uses sophisticated algorithms to compare the energy consumption recorded by the IPEM with the expected consumption based on the distribution network's load profile.

3. Utility Control Server aggregates data from multiple IPEMs and IPTD units. It performs real-time analysis by generating alerts and reports for detected theft attempts. Radio Frequency (RF) and GSM networks facilitate communication between the server and the meters.

Energy Meter with Integrated GSM Theft Detection and Automation. Authors [11] proposed using an automatic energy meter system with an intelligent energy meter sensor connected to the power lines, interfaced with a microcontroller and GSM module. This system continuously monitors power consumption and compares it with stored data in the flash memory. Any discrepancies between the recorded and monitored values indicate theft, prompting the system to send an SMS alert to the electricity board. The system's microcontroller ensures accurate theft detection to monitor real-time power consumption.

Comparison and Contribution of the Present Study

The reviewed study provides various approaches to detecting electricity theft while focusing on estimated consumption patterns that may indicate theft. While these methods have proven useful, they often rely on post-event analysis or indirect measures. Some of this may not always reflect on theft occurrences, as the legitimate consumption spikes can sometimes be misinterpreted as theft.

METHODOLOGY

This section outlines the research methodologies and materials used in developing and implementing the intelligent prepaid energy meter system. These methodologies cover the design, modelling, and testing phases.

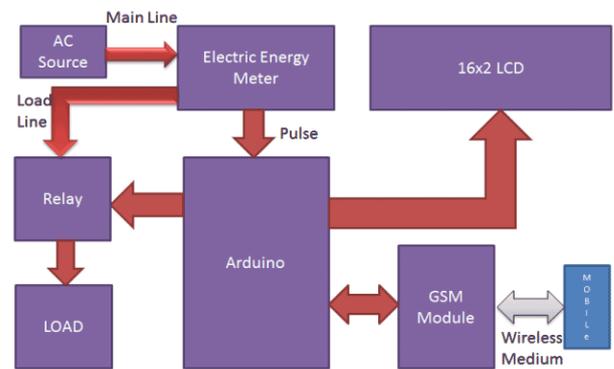


Figure 2 – Block Diagram of Prepaid Energy Meter using GSM

The design methodology is segmented into the following components:

- 1) System Design and Modeling;
- 2) Circuit Design: Power Supply Circuit and Metering Circuit;
- 3) Detection Mechanisms: Energy Theft and Meter Bypass Detection Circuits;
- 4) Microcontroller Programming: Firmware Development;
5. Energy Management and Communications.

The design phase involves creating a block diagram to outline the power supply, metering circuits, detection mechanisms, microcontroller, energy management and communication modules.

Based on the requirements, appropriate components were selected for each part of the system.

Power Supply Circuit. The LCD microcontroller and relay operate on a 12VDC power supply. The mains power supply of 240V-220V AC is stepped down to 12VAC using a 240V-220V/12V step-down transformer. A bridge rectifier is used to convert the 12VAC to 12VDC. A high-capacity capacitor (1000 μ F) smooths out any voltage ripples. The GSM SIM 800 module is essential for communication. And it requires a 4.2VDC supply. This voltage is regulated using an LM317 adjustable voltage regulator.

Metering Circuit. The metering circuit comprises voltage and current sensing circuits, crucial for measuring power consumption. It includes designing current-sensing circuits with transformers and voltage-sensing circuits with resistive dividers.

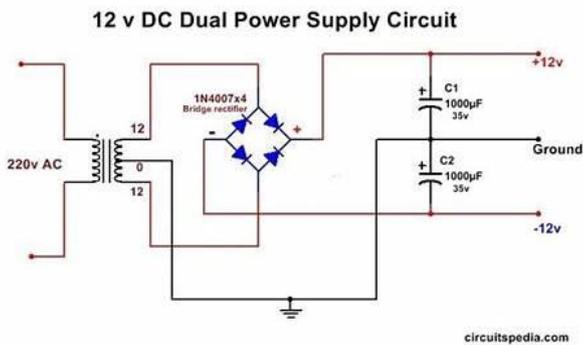


Figure 3 – 240V-220V to 12V Power Supply Circuit

They are used to monitor the current that is being drawn by the load. And the voltage supplied that allows for accurate power calculation and consumption measurement.

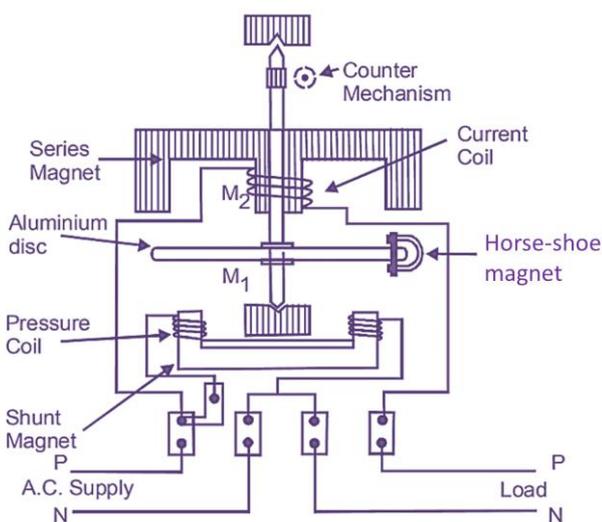


Figure 4 – Single-Phase Energy Meter

Current Sensing Circuit. A bar-type primary current transformer with a 1,000:1 transformation ratio measures the AC circuit. The output from the current transformer is connected to the microcontroller's Analog Digital Converter (ADC) pin. A 220-ohm resistor is placed across the current transformer's secondary terminals. The microcontroller measures the peak-to-peak voltage across this resistor and computes the current using Ohm's law ($V = I \times R$). The current's root mean square (RMS) value is then calculated by multiplying the measured current by 0.707 and adjusting the transformation ratio to obtain the actual primary current.

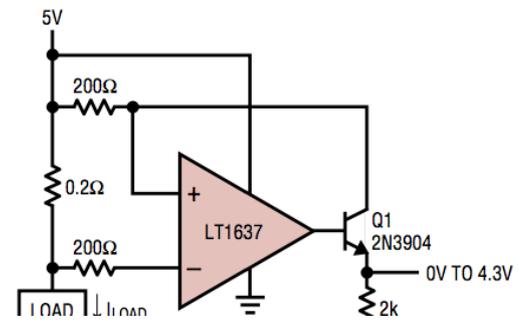


Figure 5 – Current Sensing Circuit [23]

Voltage Divider Circuit. The voltage across the load is measured using a voltage sensor connected across the main supply, and its output is connected to the microcontroller. The voltage sensor operates based on a voltage divider circuit, which scales the voltage to a level the microcontroller's ADC can safely handle. The circuit consists of two resistors: 14Ω (R1) on the live wire and another 10kΩ (R2) on the neutral wire, as shown below.

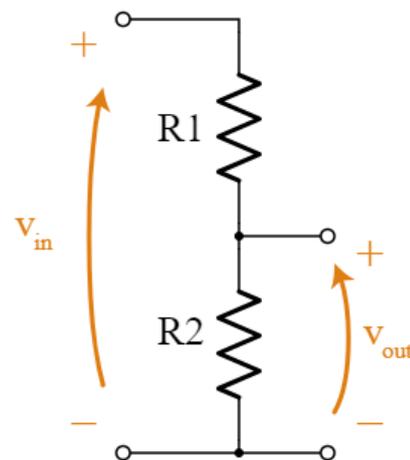


Figure 6 – Voltage Divider Circuit

Calculation of Voltage Divider Circuit. The Input Voltage from the primary side of the transformer, $V_{IN} = 220V$. To convert the 220VAC input voltage from the primary side of the transformer to a lower voltage level that the Arduino can safely measure, we need to step down the voltage using a voltage-sensing circuit. This involves a step-down transformer to reduce the AC voltage and scale to a level the Arduino can handle.

The voltage divider formula is given by:

$$V_{out} = V_{in} \left(\frac{R_2}{R_1 + R_2} \right), \tag{1}$$

V_{in} is the input voltage after rectification. The DC Voltage is 12VDC.

Assume V_{out} is 5VDC since we are using Nano Arduino, and the suitable voltage that can be accommodated is 0-5V.

$$5V = 12V \left(\frac{R_2}{R_1 + R_2} \right), \quad (2)$$

$$\frac{5}{12} = \frac{R_2}{R_1 + R_2}, \quad (3)$$

$$R_1 = R_2 \left(\frac{12}{5} - 1 \right), \quad (4)$$

$$R_1 = R_2 \left(\frac{7}{5} \right). \quad (5)$$

Choosing R_2 as a standard resistor value 10K Ω

$$R_1 = 10K\Omega \left(\frac{7}{5} \right), \quad (6)$$

$$R_1 = 10\Omega * 1.4, \quad (7)$$

$$R_1 = 14K\Omega, \quad (8)$$

Since $R_1 = 6.6K\Omega$ and $R_2 = 4.7K\Omega$

$$V_{out} = V_{in} \left(\frac{R_2}{R_1 + R_2} \right), \quad (9)$$

$$V_{out} = 12V \left(\frac{10K\Omega}{14\Omega + 10K\Omega} \right), \quad (10)$$

$$V_{out} = 12V \left(\frac{10K\Omega}{24K\Omega} \right), \quad (11)$$

$$V_{out} = 12V * 0.42 \quad (12)$$

$$V_{out} = 5V. \quad (13)$$

Arduino Code Analysis

```
const int sensor Pin = A0; // Analog input pin connected to
the voltage divider
```

```
float voltage = 0;
```

```
void setup() {
```

```
  Serial.begin(9600);
```

```
}
```

```
void loop() {
```

```
  int sensorValue = analogRead(sensorPin);
```

```
  voltage = sensorValue * (5.0 / 1023.0); // Convert analog
reading to voltage
```

```
  Serial.print("Measured Voltage: ");
```

```
  Serial.println(voltage);
```

```
  delay(1000);
```

```
}
```

Pin Definition

```
const int sensor Pin = A0; // Analog input pin connected to the
voltage divider
```

The variable "sensor Pin" refers to the analogue input pin A0 on the Arduino board. This pin is connected to a voltage divider circuit, which will be used to measure the voltage.

Variable Initialization

```
float voltage = 0;
```

The 'voltage' is to store the calculated voltage.

Setup Function

```
void setup() {
```

```
  Serial.begin(9600);
```

```
}
```

The "setup()" function allows the Arduino to send data to a monitor for display.

Main Loop

```
void loop() {
```

```
  int sensorValue = analogRead(sensorPin);
```

```
  voltage = sensorValue * (5.0 / 1023.0); // Convert analog
reading to voltage
```

```
  Serial.print("Measured Voltage: ");
```

```
  Serial.println(voltage);
```

```
  delay(1000);
```

```
}
```

This "loop" function executes the read sensor value that reads the analogue voltage value from "sensorPin" (AO). It also converts to a voltage reading where the Arduino voltage is 5.0VDC, and the maximum value for ADC is 10 bits. It also shows the calculated voltage on the monitor for observation.

Energy Theft and Meter Bypass Detection Circuit.

The meter bypassing system was simulated by connecting a 100W incandescent bulb to the external current transformer. The system successfully detects the load and sends an SMS notification to the utility company.

Microcontroller Programming.

The microcontroller handles data acquisition from sensors, processes measurements, and controls the communication module. This included writing code for ADC readings, data processing, and theft detection algorithms.

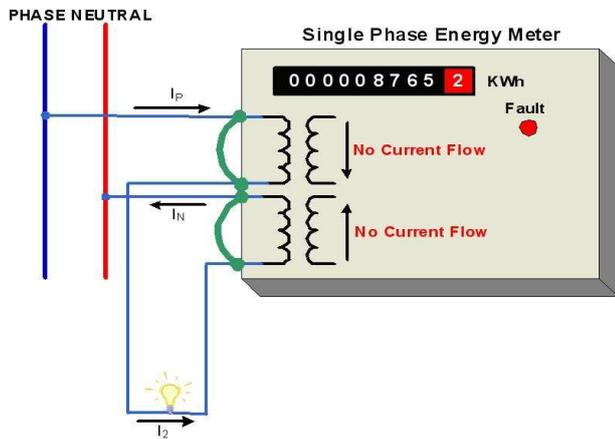


Figure 7 – Energy Meter Bypass using Bul

Energy Management and Communication. Implemented a remote access system for users to recharge energy units and monitor consumption. It involved integrating the GSM module for communication and developing an understandable interface for remote interaction.

The below-listed materials are used during this project:

Components and Equipment: 1) Microcontroller: This is used to process sensor data and control system operations using Arduino; 2) Current transformer: a bar-type transformer with a 1,000:1 transformation ratio for current measurement was used; 3) Voltage Sensor: this is used to measure voltage across the load using a voltage divider circuit; 4) GSM SIM 800 Module: this is used for communication and real-time reporting; 5) Power Supply Components include a 240V-220V/12V transformer, bridge rectifier, capacitors, and LM317 voltage regulator; 6) Resistors: this is used for voltage divider circuits and current sensing.

Software Tools: 1) Programming Environment: Arduino IDE (Integrated Development Environment) was used for microcontroller programming; 2) Simulation Tools: Software for circuit simulation and design validation, such as LTspice or Proteus.

Testing Instruments: 1) Multimeter: This is used to measure voltage, current, and resistance; 2) Oscilloscope: This is used to analyze waveforms and verify signal integrity; 3) Power Analyzer: This is used to evaluate power consumption and efficiency.

Documentation and References: 1) Technical manuals and datasheets for components and modules used; 2) Research papers and articles

related to energy theft detection and meter tampering for background and comparative analysis.

RESULTS AND DISCUSSION

The system was simulated using Proteus software and Fritzing. The Arduino Nano was programmed using the Arduino Integrated Development Environment (IDE) on a Windows 11 operating system. The programming was done in C language.

The testing process was conducted in several stages:

Unit Testing. Individual components of the energy metering system, including transformers and relays, were tested to verify their functionality. This involved ensuring that the transformers provided the correct voltage and that the relays operated correctly.

Power Supply Section Testing. The power supply unit, comprising a step-down transformer, bridge rectifier, and smoothing capacitor, was tested to confirm that it provided the required voltage levels.

Metering Circuit Testing. The metering circuit, which includes voltage and current sensing components, was tested for accuracy. Known load values were connected, and the readings were compared with the meter's display on the LCD. For instance, a 60-W incandescent bulb was tested, with the meter reading 58.42W, which is within an acceptable range.

Energy Meter Bypassing Testing. Meter bypassing was simulated by connecting an additional 60-W incandescent bulb after the external current transformer. The system detected the additional load and sent an SMS notification to the utility.

Meter Tampering Testing. Tampering was tested by opening the meter casing, which activated the momentary switch. The pre-registered utility number received an SMS notification of the tampering event.

Energy Management Testing. Energy management was tested by sending "OFF" and "ON" commands via SMS to the GSM module. The relay correctly disconnected and reconnected the load based on these commands. The system also allowed users to check the energy meter status by sending "STATUS" via SMS.

Prepayment System Testing. The prepayment functionality was tested by sending a recharge SMS in the format *333*(4 digits), where the four digits represent the desired energy units. Successfully recharges updated energy units, while unsuccessful attempts trigger notifications to the user.

CONCLUSIONS

This project successfully designed, implemented, and tested a Smart Prepaid Energy Metering

System capable of detecting energy theft through meter bypassing and tampering. The system's combination of advanced features marks a significant advancement in energy metering technology. The method efficiently solves the issue of electricity theft, which accounts for significant non-technical losses in power distribution. The results show that the system reliably measures energy consumption and detects unauthorized activities. It also provides remote management capabilities, making it a complete solution for improving power sector efficiency.

REFERENCES

1. Mohammad, N., Barua, A., & Arafat, M. A. (2013). A smart prepaid energy metering system to control electricity theft. *2013 International Conference on Power, Energy and Control (ICPEC)*, 562–565. doi: [10.1109/icpec.2013.6527721](https://doi.org/10.1109/icpec.2013.6527721)
2. Dineshkumar, K., Ramanathan, P., & Ramasamy, S. (2015). Development of ARM processor based electricity theft control system using GSM network. *2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015]*. doi: [10.1109/iccpct.2015.7159401](https://doi.org/10.1109/iccpct.2015.7159401)
3. Etukudor, C., Abdulkareem, A., & Ayo, O. (2015). *Daunting Challenges of the Nigerian Electricity Supply Industry*. *Journal of Energy Technologies and Policy*, 5, 25–32.
4. Mbunwe, M. J., David, N. (2016). *Curtailing Energy Theft by Remote Monitoring Case study: University of Nigeria, Nsukka*. Retrieved from https://www.researchgate.net/publication/311273383_Curtailing_Energy_Theft_by_Remote_Monitoring_Case_study_University_of_Nigeria_Nsukka
5. Hashmi, Md. U., & Priolkar, J. G. (2015). Anti-theft energy metering for smart electrical distribution system. *2015 International Conference on Industrial Instrumentation and Control (ICIC)*, 1424–1428. doi: [10.1109/iic.2015.7150972](https://doi.org/10.1109/iic.2015.7150972)
6. Eseosa, O., & Promise, E. (2015). *Economic Effect of Technical and Non-Technical Losses in Nigeria*. Retrieved from https://www.researchgate.net/publication/273261056_Economic_Effect_of_Technical_and_Non_Technical_Losses_in_Nigeria_Power_Transmission_System
7. Okokpujie, K., Abayomi-Alli, A., Abayomi-Alli, O., Odusami, M., Okokpujie, I., & Akinola, O. (2017). *An automated energy meter reading system using GSM technology*. Retrieved from https://www.researchgate.net/profile/Imhade-Okokpujie/publication/323390254_AN_AUTOMATED_ENERGY_METER_READING_SYSTEM_USING_GSM_TECHNOLOGY/links/5a930320a6fdccceff059a84/AN-AUTOMATED-ENERGY-METER-READING-SYSTEM-USING-GSM-TECHNOLOGY.pdf
8. Alrashed, F., & Asif, M. (2014). Trends in Residential Energy Consumption in Saudi Arabia with Particular Reference to the Eastern Province. *Journal of Sustainable Development of Energy, Water and Environment Systems*, 2(4), 376–387. doi: [10.13044/j.sdewes.2014.02.0030](https://doi.org/10.13044/j.sdewes.2014.02.0030)
9. Omijeh, B., Ighalo, G., & Anyasi, F. (2012). *Intelligent Power Theft Detection Model for Prepaid Energy Metering in Nigeria*. Retrieved from https://www.researchgate.net/publication/264496030_Intelligent_Power_Theft_Detection_Model_for_Prepaid_Energy_Metering_In_Nigeria
10. Malhotra, P., & Seethalakshmi, R.. (2013). *Automatic meter reading and theft control system by using GSM*. Retrieved

https://www.researchgate.net/publication/293249103_Automatic_Meter_Reading_and_Theft_Control_System_by_Using_GSM

11. Fan, Y., Chen, J., Bian, Q., Wu, Y., Tong, J., & Zhan, C. (2024). Design of maximum power point energy storage and inverter for photovoltaic power generation. *Journal of Physics: Conference Series*, 2771(1), 012018. doi: [10.1088/1742-6596/2771/1/012018](https://doi.org/10.1088/1742-6596/2771/1/012018)
12. Tyler, D. (1997). *Electrical Power Technology*. N. d. : Routledge.
13. Yang, Z., Wang, Y., Chen, J., & Zhou, Z. (2023). Smart Meter Fault Diagnosis based on Directional Gradient KNN. *2023 5th International Conference on System Reliability and Safety Engineering (SRSE)*, 8–13. doi: [10.1109/srse59585.2023.10336055](https://doi.org/10.1109/srse59585.2023.10336055)
14. Cameron, N. (2023). *Electronic Projects with the ESP8266 and ESP32*. Retrieved from <https://link.springer.com/book/10.1007/978-1-4842-6336-5>
15. Bais, V., Dongre, K., Bhagat, A. P., Khodke, P. A., & Ali, M. S. (2016). Network analysis model based on canny communication system for theft detection. *2016 Online International Conference on Green Engineering and Technologies (IC-GET)*, 9, 1–6. doi: [10.1109/get.2016.7916720](https://doi.org/10.1109/get.2016.7916720)
16. Gupta, A. K., Routray, A., & Naikan, V. A. (2020). Detection of Power Theft in Low Voltage Distribution Systems: A Review from the Indian Perspective. *IETE Journal of Research*, 68(6), 4180–4197. doi: [10.1080/03772063.2020.1787881](https://doi.org/10.1080/03772063.2020.1787881)
17. N. d. (2023). Data Analytics for Smart Grids Applications — A Key to Smart City Development. (2023). In D. Kumar Sharma, R. Sharma, G. Jeon, & R. Kumar (Eds.), *Intelligent Systems Reference Library*. Springer Nature Switzerland. doi: [10.1007/978-3-031-46092-0](https://doi.org/10.1007/978-3-031-46092-0)
18. Smith, T. B. (2004). Electricity theft: a comparative analysis. *Energy Policy*, 32(18), 2067–2076. doi: [10.1016/s0301-4215\(03\)00182-4](https://doi.org/10.1016/s0301-4215(03)00182-4)
19. International Energy Agency. (N. d). Looking for something? Retrieved from <https://www.iea.org/stas/index.asp>
20. Ayyub, I. (2017, April 29). *Prepaid Energy Meter using GSM and Arduino*. Retrieve from <https://duino4projects.com/prepaid-energy-meter-using-gsm-arduino/>
21. User Manual and Diagram Library. (2024, March 24). *12v Power Schematic Wiring*. Retrieved from <https://enginedataemitting.z22.web.core.windows.net/12v-power-schematic-wiring.html>
22. Electrical WorkBook. (2021, July 12). *Single Phase Energy Meter – Working, Construction & Diagram*. Retrieved from <https://electricalworkbook.com/single-phase-energy-meter/>
23. Embedded Lab. (2014, May 21). Techniques of current sensing. Retrieved from <https://embedded-lab.com/blog/tag/current-sensor>