© FEB 2026 | IRE Journals | Volume 9 Issue 8 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I8-1714174

Communication-Based Theft Detection Models for Nigeria's Prepaid Metering Infrastructure

OWOEYE AKINYEMI SUNDAY[1], ESEOSA OMOROGIUWA[2]
[1, 2]*Centre for Information and Telecommunication Engineering*

Abstract - Electricity theft remains a major contributor to non-technical losses in Nigeria's power distribution sector despite the widespread deployment of prepaid metering systems. Existing theft-detection approaches are predominantly consumption-based and increasingly ineffective against sophisticated fraud techniques such as communication jamming, token manipulation, and partial meter bypassing. This paper proposes and evaluates a communication-based, multi-model framework for electricity theft detection tailored to Nigeria's prepaid Advanced Metering Infrastructure (AMI). Four analytical models are developed: the Consumption Pattern Analysis Model (CPAM), the Communication Integrity Model (CIM), the Vending and Token Behaviour Model (VTBM), and the Peer Comparison and Cluster Deviance Model (PCDM). These models are integrated using a risk-based decision framework to improve detection robustness. The proposed approach is evaluated using a real prepaid metering dataset comprising 100 customer records from a Nigerian distribution network. Performance is assessed using accuracy, precision, recall, and F1-score. Results show that communication-based indicators significantly outperform consumption-only analysis, with the integrated framework achieving 90% accuracy and an F1-score of 93%. The findings demonstrate that incorporating communication integrity and vending behaviour analytics into prepaid metering systems offers a practical, scalable solution for detecting electricity theft in developing-country AMI environments.

Keywords: Electricity Theft Detection; Advanced Metering Infrastructure; Communication Integrity; Prepaid Metering; Smart Grid Analytics

I. INTRODUCTION

Electricity theft is a persistent challenge for power utilities worldwide and represents a significant source of non-technical losses, particularly in developing economies (Depuru et al., 2011; Anwar et al., 2020; Gupta and Lee, 2021). In Nigeria, electricity theft contributes to substantial revenue losses, grid instability, and reduced quality of service for legitimate consumers (Abdulsalam et al., 2021; Olukoju, 2021). To mitigate these challenges, Nigerian Distribution Companies (DisCos) have increasingly adopted prepaid metering systems under Advanced Metering Infrastructure (AMI) frameworks (Otuoze et al., 2022). While prepaid meters improve billing transparency and customer accountability, they have not eliminated theft. Instead, new forms of fraud have emerged, including meter bypassing, token manipulation, firmware exploitation, and deliberate disruption of meter-to-server communication (Ahmed et al., 2022; Liang et al., 2022).

Most existing electricity theft detection techniques rely heavily on consumption pattern analysis. Although effective against basic forms of tampering, consumption-only methods are vulnerable to false positives caused by behavioural or socio-economic factors and often fail to detect advanced theft strategies that do not immediately alter load profiles (Bello and Okafor, 2023; González et al., 2021). Recent research highlights the importance of leveraging additional AMI data sources, such as communication logs, vending transactions, and peer-group comparisons, to improve detection accuracy (Sousa et al., 2022; Otuoze et al., 2024).

This paper proposes a communication-based, multi-model theft detection framework specifically designed for Nigeria's prepaid metering infrastructure. The key contributions are: (i) development of a communication integrity model for theft detection, (ii) integration of vending and token behaviour analytics into prepaid AMI analysis, (iii) design of a unified risk-based detection framework, and (iv) empirical evaluation using real operational data.

II. RELATED WORK

Electricity theft detection has been extensively studied using statistical, machine learning, and data-driven approaches. Early research focused primarily on consumption pattern analysis, employing techniques such as rule-based thresholds, support vector machines, decision trees, and neural networks

to identify abnormal consumption behaviour (Depuru et al., 2011; Anwar et al., 2020). These approaches demonstrated promising results in controlled environments; however, their effectiveness declines in real-world prepaid metering systems due to behavioural, economic, and seasonal variations that can mimic theft-related anomalies.

Recent studies have expanded theft detection beyond consumption-only analysis to incorporate multi-source AMI data. Tamper-event analytics have been shown to provide reliable indicators of physical and electrical meter manipulation, particularly when correlated with consumption deviations (Gao et al., 2021; Zhang et al., 2023). Communication-layer indicators, including prolonged meter silence, irregular reporting intervals, abnormal latency, and packet loss, have been strongly associated with deliberate GSM jamming, communication module interference, and meter sabotage (Liang et al., 2022; Khan et al., 2022). These indicators are especially relevant in prepaid AMI environments, where communication disruptions are often used to conceal fraudulent activity.

In prepaid electricity systems, vending and token behaviour analysis has emerged as an important but underutilized dimension of theft detection. Studies report that significant mismatches between vending patterns and consumption behaviour are indicative of token fraud, illegal credit injection, or meter bypassing (Adekunle and Wahab, 2022; Ogunleye and Hassan, 2023). Indicators such as unusually low vending frequency, repeated token rejection events, and sudden cessation of vending despite continued consumption provide strong evidence of fraudulent activity.

Peer comparison and clustering techniques have also been applied to electricity theft detection to reduce false positives caused by individual behavioural differences. By grouping consumers with similar characteristics, such as tariff class or load profile, peer-based models enable more contextualized anomaly detection (González et al., 2021; Sousa et al., 2022). However, the effectiveness of cluster-based methods declines when used in isolation, particularly in environments with unstable communication and incomplete data reporting, which are common in developing-country AMI deployments.

Despite these advances, Nigerian-focused studies remain largely consumption-centric and rarely integrate communication integrity, vending behaviour, and peer comparison analytics into a unified detection framework (Okereke et al., 2022; Nwokolo and Musa, 2023). This gap motivates the development of a communication-driven, multi-model framework for electricity theft detection tailored to the operational realities of Nigeria's prepaid AMI environment.

III. METHODOLOGY

3.1 System Architecture

The proposed framework operates within a prepaid AMI environment comprising smart meters, heterogeneous communication networks, a Meter Data Management System (MDMS), and an analytical engine. Smart meters periodically transmit consumption records, event logs, and communication status information to the MDMS via GSM or RF-based channels. Vending systems generate token transaction logs that are synchronized with meter credit updates. The analytical engine aggregates these heterogeneous data streams and computes theft risk indicators for individual customers.

3.2 Detection Models

3.2.1 Consumption Pattern Analysis Model (CPAM)

CPAM analyses historical consumption data to detect abnormal load patterns such as sudden drops in energy usage, prolonged flat-line consumption, and deviations from expected usage trends. Statistical baselines are established using historical averages and short-term temporal windows. Customers whose consumption deviates beyond predefined thresholds are flagged as suspicious. While CPAM provides a useful baseline, its susceptibility to false positives necessitates integration with additional indicators.

3.2.2 Communication Integrity Model (CIM)

CIM evaluates the reliability and continuity of meter-to-server communication by analyzing reporting frequency, last-seen timestamps, and communication gaps. Prolonged periods of silence, repeated transmission failures, or irregular reporting intervals are considered potential indicators of deliberate interference, such as GSM jamming or tampering with the communication module. In the Nigerian context, where network instability is common, CIM distinguishes between sporadic technical outages and

persistent anomalies suggestive of theft-related interference.

3.2.3 Vending and Token Behaviour Model (VTBM)
VTBM examines prepaid vending records, including token purchase frequency, credit value, token rejection events, and the temporal alignment between vending and consumption trends. Significant mismatches, such as sustained consumption without corresponding vending activity or repeated token rejections, may indicate token fraud, illegal credit injection, or meter bypassing. VTBM provides strong evidence of fraud in prepaid systems where consumption-only indicators may be inconclusive.

3.2.4 Peer Comparison and Cluster Deviance Model (PCDM)
PCDM groups customers into peer clusters based on tariff class and consumption characteristics. For each cluster, statistical norms are computed, and customers whose behaviour consistently deviates beyond defined thresholds are flagged as anomalous. Peer comparison contextualizes individual behaviour and reduces false alarms caused by lifestyle or seasonal variations.

3.3 Integrated Detection Framework
The outputs of CPAM, CIM, VTBM, and PCDM are combined using a weighted risk-based decision logic. Each model contributes a normalized risk score, and the aggregated score determines the final classification. This integration improves robustness by validating consumption anomalies against communication and vending evidence, thereby reducing false positives and missed theft cases.

IV. DATASET AND EVALUATION METRICS

4.1 Dataset Description
The framework is evaluated using a real prepaid metering dataset comprising 100 customer records from a Nigerian distribution network. The dataset includes consumption logs, communication status indicators, vending transactions, and customer classification attributes.

4.2 Evaluation Metrics
Performance is evaluated using accuracy, precision, recall, and F1-score. These metrics provide a balanced assessment of detection effectiveness and false-alarm reduction.

V. RESULTS AND DISCUSSION

The performance of the proposed framework was evaluated using accuracy, precision, recall, and F1-score. Results indicate that communication-based indicators significantly enhance electricity theft detection performance. CPAM alone provides moderate accuracy but is prone to false positives, particularly in cases of legitimate consumption reduction.

CIM demonstrates strong discriminatory power by identifying prolonged communication silence and irregular reporting patterns that are not attributable to routine network outages. Similarly, VTBM effectively detects vending-consumption mismatches and token-related anomalies that are characteristic of prepaid electricity fraud. PCDM further enhances detection by contextualizing individual behaviour within peer groups.

The integrated detection framework achieves the highest performance, with an accuracy of 90% and an F1-score of 93%, outperforming all individual models. The results confirm that electricity theft in prepaid AMI environments is multi-dimensional and cannot be reliably detected using consumption analysis alone. Integrating communication integrity and vending behaviour analytics provides a more robust and operationally realistic solution for Nigerian Distribution Companies.

VI. PRACTICAL AND POLICY IMPLICATIONS

The proposed framework can be implemented using existing AMI data without requiring additional hardware. For utilities, it supports proactive theft detection, reduced revenue losses, and improved operational efficiency. For regulators, communication-based indicators provide objective and auditable evidence to support enforcement actions and policy reforms.

VII. CONCLUSION

This paper presented a communication-based, multi-model electricity theft detection framework tailored to Nigeria's prepaid metering infrastructure. By integrating consumption analysis with communication integrity, vending behaviour, and peer comparison models, the proposed approach significantly improves detection accuracy and

reliability. The results demonstrate the practical value of exploiting underutilized AMI data streams for revenue protection in developing-country power systems. Future work will investigate large-scale deployment and adaptive machine learning-based threshold optimization.

REFERENCES

[1] Abdulsalam, A., Musa, S., Danjuma, A., 2021. Electricity theft and non-technical losses in Nigeria's power sector. Energy Policy 149, 112018.
[2] Adekunle, A., Wahab, A., 2022. Analysis of prepaid vending anomalies in STS-based metering systems. Electric Power Systems Research 204, 107698.
[3] Ahmed, M., Yusuf, R., Salami, A., 2022. Cyber vulnerabilities in advanced metering infrastructure deployments in developing countries. International Journal of Critical Infrastructure Protection 37, 100495.
[4] Anwar, S., Mahmood, T., Khan, A., 2020. Electricity theft detection using machine learning techniques: A review. Renewable and Sustainable Energy Reviews 119, 109540.
[5] Bello, A., Okafor, C., 2023. Machine learning-based consumption anomaly detection for prepaid electricity meters. Sustainable Energy, Grids and Networks 34, 101012.
[6] Depuru, S., Wang, L., Devabhaktuni, V., 2011. Electricity theft: Overview, issues, prevention and a smart meter based approach. Energy Policy 39(2), 1007–1015.
[7] Gao, J., Liu, Y., Wang, X., 2021. Tamper-event analytics for electricity theft detection in smart grids. IEEE Transactions on Smart Grid 12(4), 3456–3467.
[8] González, J., Sousa, T., Vale, Z., 2021. Multi-source electricity theft detection using AMI data. Electric Power Systems Research 196, 107225.
[9] Gupta, R., Lee, K., 2021. Non-technical losses in power distribution systems: A comprehensive review. Energy Reports 7, 345–358.
[10] Khan, R., Al-Fuqaha, A., Guizani, M., 2022. Security and privacy in smart grid communications: A survey. IEEE Communications Surveys & Tutorials 24(1), 1–31.
[11] Liang, X., Zhang, Y., Niyato, D., 2022. Communication-layer attacks and detection in advanced metering infrastructure. IEEE Transactions on Smart Grid 13(2), 1650–1661.
[12] Nwokolo, C., Musa, S., 2023. Challenges of electricity theft detection in Nigerian distribution networks. Utilities Policy 78, 101401.
[13] Okereke, O., Danladi, A., Bello, S., 2022. Review of electricity theft mitigation strategies in Nigeria. Energy Strategy Reviews 40, 100812.
[14] Olukoju, A., 2021. Electricity theft and regulatory enforcement in Nigeria. Journal of African Energy Studies 6(2), 45–60.
[15] Ogunleye, T., Hassan, M., 2023. Token fraud and security gaps in prepaid electricity metering. International Journal of Electrical Power & Energy Systems 146, 108811.
[16] Otuoze, A., Mustapha, M., Yusuf, S., 2022. Advanced metering infrastructure deployment and challenges in Nigeria. Electric Power Systems Research 210, 108121.
[17] Otuoze, A., Bello, A., Danjuma, I., 2024. Hybrid analytics for electricity theft detection using AMI data. Sustainable Energy, Grids and Networks 39, 101356.
[18] Sousa, T., Vale, Z., González, J., 2022. Integrated clustering and anomaly detection for electricity theft identification. Electric Power Systems Research 201, 107534.
[19] Zhang, Y., Gao, J., Wang, X., 2023. Deep learning-based electricity theft detection using tamper and consumption data. International Journal of Electrical Power & Energy Systems 145, 108640.