JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 12(3), SEPTEMBER, 2024
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

Enhanced Theft Mitigation on Electrical Power using Smart Metering Infrastructure

Oguche Emmanuel Ojochenemi, Eronu Emmanuel Majiyebo
Electrical/Electronic Engineering Department,
Faculty of Engineering. University of Abuja.

ABSTRACT
Electricity theft remains a significant challenge for power distribution networks worldwide, particularly in regions with limited enforcement and out-dated infrastructure. This illicit activity results in substantial financial losses, operational inefficiencies, and compromised grid reliability, ultimately impacting both utility companies and honest consumers. Traditional methods of detecting electricity theft, such as physical inspections and manual audits, have proven insufficient in addressing increasingly sophisticated theft techniques. However, advancements in smart metering infrastructure offer new possibilities for enhancing theft detection and mitigation. This paper explores the development of an enhanced theft mitigation strategy leveraging smart metering technology to detect and prevent unauthorized electricity consumption more effectively. The study proposes a comprehensive framework of developed algorithm which was implemented using python programming and the algorithm's performance evaluated under different conditions and parameter such as intrusion detection status which monitors whether the metre is powered on or powered off, Time step error which is the error in monitoring the progression of electricity supply to customers at regular increments, real time pricing plays a crucial role in identifying deviations in the price of electricity, the central observer metre status which checks if the power supply at the source corresponds to the total sum of electricity supplied to customers, accounting for expected technical losses. This Model is validated by comparing it's predictions with observations from real field data collected from AEDC Bwari Abuja. Data's of a sample size of 98 customer meters were collected and the validation step showed that greater than 83% prediction accuracy of the model to respect with the real data.

ARTICLE INFO
Article History
Received: June, 2024
Received in revised form: June, 2024
Accepted: July, 2024
Published online: September, 2024

KEYWORDS
Theft Mitigation, Electrical Power, Smart Metering

INTRODUCTION

Electricity is a basic human resource that is essential for the smooth running of human activities and a driver of a nation's economy [1]. Due to the indispensable nature of this resource, it is critical to effectively manage its generation, distribution, supply, and consumption, as failure to effectively optimize these processes usually results in the malfunctioning of various systems of society, especially the economy. According to Dahunsi *et al*. [2], Nigeria has about 45% electrification capacity (144 kWh/capita), which lags behind other African counterparts such as South Africa (84.4%), Ghana (83%), and Kenya (64%). With a total installed capacity of 16,384 MW, Nigeria has three (3) hydro plants and 22 gas plants producing 2,062 MW and 11,972 MW, respectively, while wind, solar, and others (diesel, hydrofluorocarbons) account for 10 MW, 7 MW, and 2,333 MW, respectively [3]. Nigeria currently has an available generating capacity of about 9,000 MW and a transmitting capacity of 5,300

Corresponding author: Oguche Emmanuel Ojochenemi.
✉ *ogucheeo@gmail.com*
Electrical/Electronic Engineering Department, University of Abuja.

MW for a 20,000 km transmission coverage across the nation. However, with just 25% of potential energy reaching only about 60% of the population, the country is obviously plagued with the challenge of electricity shortage [4].Power shortage is endemic to Nigeria, and a major contributor to this shortage is electricity theft. As highlighted by Dike *et al*. [5], Nigeria's electricity distribution companies (DisCos) continue to report worrying losses in electricity theft, which account for huge revenue losses. As a result, the power sector has been short of quality investment and adequate infrastructure. There has also been poor management, all of which have led to a chronic shortage in electricity supply [6]. To address these problems, the government decided to privatize the power sector in 2013, to improve power generation and distribution [7]. However, this approach has had its associated challenges. For instance, recent reports from the Nigerian Electricity Regulatory Commission (NERC) reveal that the eleven (11) DisCos operating in Nigeria's electricity industry are incurring substantial losses, estimated to be as much as 47.9% of the total value of energy sold [8]. Kambule *et al*. [9] also report that overall, Nigeria has recorded over $54 billion loss in electricity theft to date. These huge financial losses continue to bedevil the country's already anaemic power sector and economy. The consequent effects have led to substantial losses in revenue for the government and a lack of investment in the power sector. The challenge of electricity theft in Nigeria is a multifaceted issue that is influenced by several factors ranging from poverty, unemployment, and lack of efficiency in the supply of electricity [10], [11]. In many cases, individuals resort to stealing electricity as a means of obtaining power, especially in areas where the grid is unreliable or non-existent [11]. Additionally, organized criminal groups are involved in electricity theft, which often involves bypassing meters or stealing power directly from the grid.

To this end, the smart metering technology has been proposed as a viable solution to the problem of electricity theft in Nigeria [12], [14]. The technology uses the Advanced Metering Infrastructure (AMI) to remotely monitor and manage energy consumption [15]. This innovation can detect and deter theft by identifying abnormal usage patterns and alerting utility companies to potential issues [16]. Despite the potential benefits of smart metering systems, their implementation in Nigeria has been slow [17]. This is in part due to the high cost of implementation, and the lack of funding for such projects. Additionally, there are technical challenges associated with implementing smart metering systems in Nigeria, such as inadequate infrastructure and a lack of skilled personnel [18]. There is also some form of resistance from consumers who may be concerned about privacy and the cost of the new technology [19]. These challenges are further worsened by a lack of information on smart metering applications in Nigeria. Thus, this work proposes a systematic workflow for electricity theft detection using the smart metering technology in the context of Nigeria's electricity grid.

Problem Statement

The persistence of electricity theft, primarily through meter bypass and tariff manipulation, poses a significant challenge to the Nigerian power sector. As the largest economy in sub-Saharan Africa, Nigeria's economic growth is undermined by its struggling energy sector, where substantial revenue losses result from both technical and non-technical inefficiencies, with theft being a leading factor. Electricity theft leads to considerable revenue loss for distribution companies (DisCos), who report losing up to half of their potential revenue from distributed electricity. These losses not only strain the financial health of DisCos but also weaken the stability and reliability of the national grid. This, in turn, affects customer satisfaction, as legitimate consumers face higher prices and inconsistent supply. Addressing electricity theft is crucial to improving energy security, boosting revenue for utilities, and supporting Nigeria's broader economic development. Smart metering technology, which leverages advanced metering infrastructure (AMI) with features like two-way communication and real-time data monitoring, presents a promising solution to reduce electricity theft. However, the deployment of smart meters in

Corresponding author: Oguche Emmanuel Ojochenemi.
oguchеeo@gmail.com
Electrical/Electronic Engineering Department, University of Abuja.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 12(3), SEPTEMBER, 2024
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

Nigeria faces challenges, including high infrastructure costs, cybersecurity risks, and consumer privacy concerns. This work specifically addresses the high cost barrier by proposing a data-driven theft detection model that operates with existing meter infrastructure, reducing the immediate need for costly AMI upgrades. By using readily available smart meter data to identify tampering indicators—such as abnormal power diversion and tariff discrepancies—this model provides utilities with a reliable and cost-effective tool for detecting electricity theft. This approach enables targeted interventions, allowing utilities to protect revenue and enhance service quality without extensive infrastructural investments, thus offering a practical solution in the current Nigerian power landscape.

APPROACH METHODS

Electricity theft is a pervasive issue in power systems, leading to substantial financial losses for utility companies. To address this challenge, a proactive and intelligent monitoring system leveraging Smart Metering Infrastructure is proposed. Unlike traditional metering systems, which rely on periodic manual readings, our approach enables real-time monitoring and analysis of consumption patterns. This section outlines the methodology, presenting a general-purpose Advanced Metering Infrastructure (AMI) network and key parameters for effective theft detection. For this study, a general-purpose simplified Advanced Metering Infrastructure (AMI) network was developed as shown in Figure 1.The algorithm's performance is then evaluated and validated using synthetic and in real-time electricity theft detection data to test for system integration under various scenarios and ensure its robustness and responsiveness. Figure 1 represents a simple interconnectedness between the zone, central observer meter, and the customers, highlighting the flow of information and communication in the smart metering infrastructure.

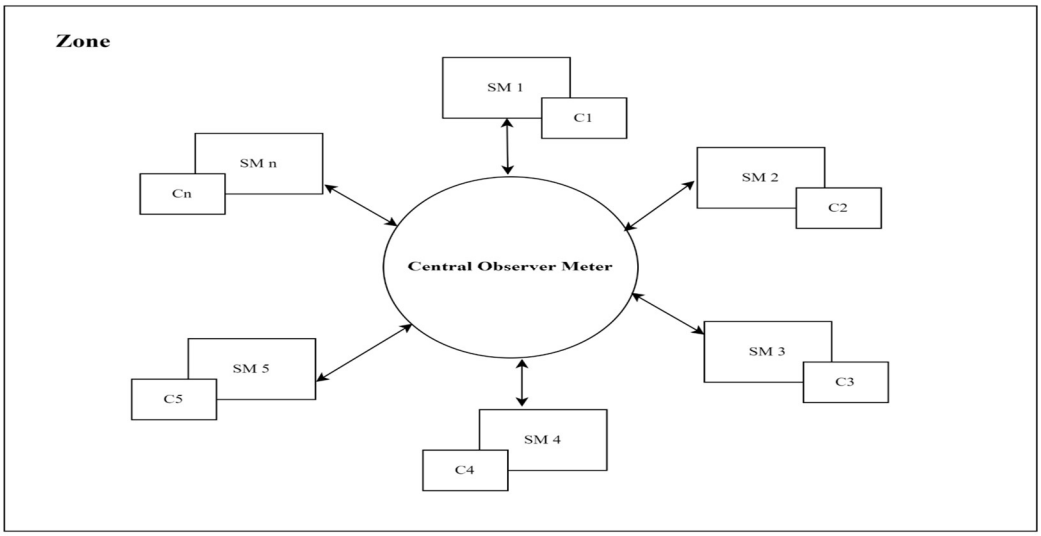

Figure 1: A Simple Interconnectedness between the Zones

Algorithm for Theft Detection

The proposed algorithm for Electricity Theft Detection operates on a Smart Metering Infrastructure. The algorithm considers various parameters, including intrusion status, timestamp error, real-time pricing error, and central observer meter status. These parameters are crucial for monitoring and detecting potential instances of theft. The algorithm follows a step-by-step logic, calculating risks associated with each customer

Corresponding author: Oguche Emmanuel Ojochenemi.
oguchеeo@gmail.com
Electrical/Electronic Engineering Department, University of Abuja.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 12(3), SEPTEMBER, 2024
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

and providing an overall measure of risk for the entire zone. We introduce parameters such as alpha (α), beta (β), gamma (γ), delta (δ), and their respective models, ensuring comprehensive monitoring.

Parameter Selection and Modelling for Electricity Theft Detection

This subsection presents the selection and modelling of parameters for the detection of electricity theft. These parameters include alpha (α), beta (β), gamma (γ), and sigma (δ), which denote the intrusion detection status, timestamp error, real-time pricing, and central observer metre status, respectively. Each parameter is key to the monitoring system and is assigned a value of 'High' for compromised states and 'Low' for uncompromised states.

The evaluation of these parameters is performed at regular timesteps represented by τ. The difference in timestamps between the current evaluation timestep (T_τ) and the previous evaluation timestep ($T_{\tau-1}$) is denoted as T_d. Thus, Equation 1 below is used to determine the constant timestep duration T_d. Therefore, any inconsistency in the value of T_d indicates an error, and flags are raised to identify potential inconsistencies in the system.

$$T_\tau - T_{\tau-1} = T_d \qquad (1)$$

Where T_τ is the timestamp at the current timestep of evaluation, $T_{\tau-1}$, the previous timestamp just before the current timestep of evaluation and Td, the difference between the two timestamps.

T_d must be constant at every timestep of evaluation for uncompromised states. Therefore, error is flagged when these values give inconsistent value of T_d. The timestamp error, β is evaluated using Eq. (2). β determines the error in the monitored timestamps and signals "High" for any inconsistency in the reported time interval within a given timestep and "Low" for normal timestamps.

$$\beta = \begin{cases} \text{Low}, & \Delta T_d = 0 \\ \text{High}, & \Delta T_d \neq 0 \end{cases} \qquad (2)$$

γ represents the deviation from the set real-time pricing by the utility to what each SEM reflects. Let p1,1, p1,2, p1,3,…, p1,τ; p2,1, p2,2, p2,3, …, p2,τ; p3,1, p3,2, p3,3,…, p3,τ; …; and pn,1, pn,2, pn,3…, pn,τ be the instantaneous real-time pricing for customers 1, 2, 3 to n applied to the neighborhood at timesteps 1, 2, 3 to τ, respectively. As presented in a previous work [83], the real-time pricing for each of the SEM can be authenticated based on Equations (3) to (5). Note that for a given neighborhood, different pricing schemes may apply to different customers depending on the type of customers and other flexible service schemes available in the SG regime. However, in this work, Eq. (3) is formulated to ensure constant monitoring of the pricing regime among customers in a zone with the assumption that all customers in a zone are subjected to an equal tariff plan at any given timestep. Equation (3) shows that the state scenario of a customer's pricing regime can be used as a check on other customers within the same zone. Equation (4) compares any given customer's pricing regime with the set value by the utility at any τ where pu,τ denotes the billing as set by the utility at timestep τ. To monitor deviation in the applied price regime to each of the customers' SEM, Eq. (5) is formulated to define the state for both compromised and uncompromised states by constantly comparing the price regimes at utility and customer ends. When a customer's pricing information is at equal state as the applied pricing by the utility, there is no suspected compromise, and the state "Low" is assumed, otherwise, the state "High" is assumed.

$$p_{1,\tau} = p_{2,\tau} = p_{3,\tau} =, \ldots = p_{n,\tau} \qquad (3)$$

$$p_{n,\tau} = p_{u,\tau} \qquad (4)$$

$$\gamma = \begin{cases} \text{Low}, & p_{n,\tau} = p_{u,\tau} \\ \text{High}, & p_{n,\tau} \neq p_{u,\tau} \end{cases} \qquad (5)$$

The inclusion of the central observer meter as provided in Fig. 2 is to provide for a real-time monitoring of all SEM in the monitored zone to determine possible abnormal deviations. The deviations in the recorded energy consumption data of each of the SEM are modelled by comparing recorded values of the central observer meter with those of the SEM in a zone. At any given timestep, energy recorded by the observer

Corresponding author: Oguche Emmanuel Ojochenemi.
ogucheeo@gmail.com
Electrical/Electronic Engineering Department, University of Abuja.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 12(3), SEPTEMBER, 2024
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

meter, E_{Ob}, and the energy recorded by all SEM in the given zone, ESEM, are monitored to determine possible compromises in each zone. The compromised or uncompromised state of the observer meter, δ, is modelled based on the value of *k* as given in Eq. (6), where k is the assumed maximum allowable unaccounted losses in a zone due to possible error in the estimation of technical losses (TL). This means the difference between the supplied energy to a zone and the reported consumption by all SEM must not be greater than k, in consideration of the TL for all uncompromised scenarios.

$$\text{TL} = \begin{cases} \text{Low}, & E_{ob} - \sum E_{SEM} \leq k \\ \text{High}, & E_{ob} - \sum E_{SEM} > k \end{cases} \quad (6)$$

Overall, the selection and modelling of these parameters ensures a comprehensive monitoring system capable of detecting and flagging potential instances of electricity theft. The models will establish baseline behaviour for each parameter and enable the identification of abnormal patterns that may indicate theft or system irregularities.

Algorithm

Input:

- $t_{\tau 1}$: Time at current time step [HH:MM:SS]
- $t_{\tau 2}$: Time at previous time step [HH:MM:SS]
- $t_{\tau 3}$: Time at two time steps back [HH:MM:SS]
- customer price (p_i): Vector of customer prices at current time step [NGN/kwh]
- utility price (p_u): Utility price of the zone at the current time step [NGN/kwh]
- E_{ob}: Energy recorded by the central observer at the current time step, accounting for expected losses [kW]
- $E_{SEM,i}$: Vector of energy recorded by customer meters in the zone at the current time step [kW]
- *k*: Maximum unaccounted losses in the zone
- $\varepsilon_1, \varepsilon_2, \varepsilon_3$: Tolerance parameters
- weights: Weights for risk calculation

Output:

- α: Vector of intrusion status for each customer
- β: Vector of time step error for each customer
- γ: Vector of real-time pricing error for each customer
- δ: Central observer meter status for the zone
- risk: Vector of electricity theft risk for each customer
- zone risk: Overall measure of risk associated with the zone

Algorithm Steps:

1. Initialize empty vectors alpha, beta, zeta, risk.
2. Iterate over each customer in the zone (*i*, from 1 to the number of customers):

a. Calculate α_i based on the comparison of $E_{SEM,i}$ with ε_1.

b. Calculate β_i based on the time difference between $t_{\tau 1}, t_{\tau 2}, t_{\tau 3}$.

c. Calculate γ_i based on the difference between customer price (p_i) and utility price (p_u).

d. Calculate $risk_i$ as the sum of β_i and γ_i.

3. Calculate sigma based on the comparison of $(E_{ob} - \sum E_{SEM})$ with *k*.

a. If verbose, print sigma.

4. Calculate the mean values of α, β, and γ.
5. Calculate zone risk using the weighted sum of the mean values from step (4).

2.2.3 Defining the Rules for Detecting Security Risks

After selecting and modelling the parameters for monitoring, we define the rules that will determine the security risks based on the possible states of each parameter. These rules are essential for the efficient implementation of the monitoring scheme and enable the identification of potential electricity theft scenarios. We formulate the following rules to define the security risks:

Using equation (4), Table 1 is then updated to Table 3.2 with δ, where the state of other parameters remains unchanged when at a "Low" state, while other rules are as captured.

Corresponding author: Oguche Emmanuel Ojochenemi.
oguchеeo@gmail.com
Electrical/Electronic Engineering Department, University of Abuja.

Table 1: Defined Rules for Security Risks

Scenario No.	α	β	γ	Security Risk
1	Low	Low	Low	Normal
2	Low	Low	High	Low
3	Low	High	Low	Low
4	Low	High	High	Medium
5	High	Low	Low	Low
6	High	Low	High	Medium
7	High	High	Low	Medium
8	High	High	High	High

Each scenario in Table 1 represents a combination of the monitored parameters, α, β, and γ. The defined rules for the security risk model indicate the corresponding security risk level for each scenario. The security risk is categorised as "Normal," "Low," "Medium," or "High" based on the combination of parameters states.

Validation

For validation purposes, field data from Ibadan Electricity Distribution Company (IBEDC) is utilized to assess the effectiveness of the proposed algorithm. The AMI network collects fine-grained data, including time-stamped measurements and load profiles, facilitating the development of sophisticated theft detection models. Synthetic data analysis is performed to evaluate consumption patterns, identify irregularities, and detect potential instances of theft. The algorithm's performance is rigorously tested to ensure accurate and timely detection.

Sensitivity Analysis

To gauge the algorithm's robustness, sensitivity studies are conducted. Parameters such as tolerance values (epsilon1, epsilon2, epsilon3) and weights for risk calculation are systematically varied. The algorithm's response to changes in these parameters is analyzed to assess its sensitivity and optimize its performance under different scenarios. Sensitivity analysis provides valuable insights into the algorithm's adaptability and reliability in diverse conditions.

Developed Electricity Theft Prevention Model Based on the Implemented Rules

The developed electricity theft prevention model implemented based on utilization of the results of the Python model for all modelled scenarios is given in Figure 2. Decisions on monitored parameters are evaluated at every time-step and are firmly based on Figure 2. If there is any risk (defined to be the "High" or "Very High" states), an attempt is made to automatically clear the threat before electricity theft is significantly committed. This adequately improves the self-healing function of the AMI. Such compromised state may necessitate further assessment or action to secure the system usually by subjecting compromised SEM to further analysis depending on if the self-healing is not able to restore the system. As shown in the developed model, further analysis may be required where automated action becomes inadequate to clear suspicious status.

Corresponding author: Oguche Emmanuel Ojochenemi.
oguchеeo@gmail.com
Electrical/Electronic Engineering Department, University of Abuja.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 12(3), SEPTEMBER, 2024
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

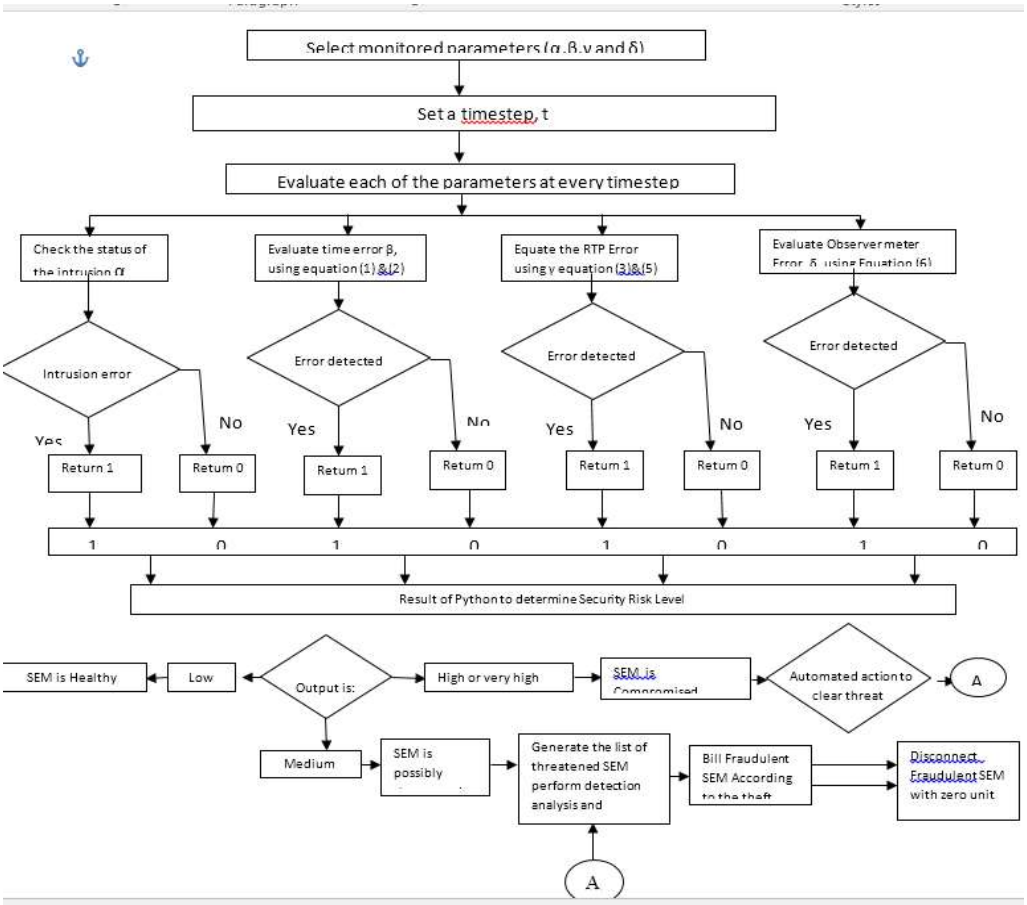

Figure 2: Developed Electricity Theft Prevention Model

RESULTS AND DISCUSSION

This section present the results of the finding and discussion. Figure 3 illustrates the sensitivity of the model's **Zone Risk** metric to variations in the weights assigned to different tampering indicators (alpha, beta, zeta, and sigma). As the weight for each indicator increases, its influence on the overall zone risk score changes, reflecting the model's flexibility to prioritize specific types of tampering based on utility requirements. For instance, increasing the **sigma** weight (red line) significantly elevates the zone risk, indicating a high sensitivity to unaccounted losses when sigma is prioritized. In contrast, increasing the weight for **alpha** (cyan dashed line) decreases zone risk, suggesting a trade-off between focusing on energy diversion (alpha) versus unaccounted losses (sigma). This analysis demonstrates that the model can be adapted to focus on particular tampering types, allowing utilities to tailor theft detection priorities according to specific operational needs.

Corresponding author: Oguche Emmanuel Ojochenemi.
ogucheeo@gmail.com
Electrical/Electronic Engineering Department, University of Abuja.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 12(3), SEPTEMBER, 2024
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

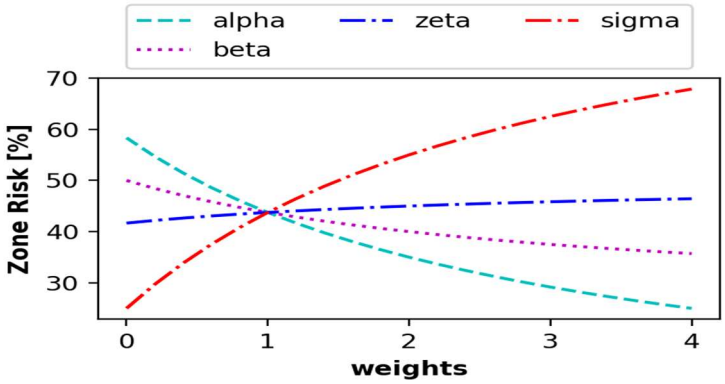

Figure 3: influence of weights on Zone risks for various parameters

REAL DATA RESULTS

Table 4.1 summarizes real-world utility data, including tariffs, current measurements, and tampering indicators for 98 meters. The **mean customer tariff** is 75.9 NGN/kWh, significantly lower than the **mean utility tariff** of 148.3 NGN/kWh, indicating frequent discrepancies. The **average incoming current** is 28.9 A, while the **outgoing current** averages 22.9 A, suggesting potential losses. Notably, around **30% of meters are flagged as tampered**. These statistics highlight the variability in tariffs, current, and tampering, which the model seeks to detect effectively. Table 2 presented the data collected.

Table 2: Summary of real meter data collected from Abuja

index	TARRIF ON METER (NGN/kWh)	ACTUAL TARRIF (NGN/kWh)	INCOMING CURRENT	OUTGOING CURRENT	TAMPERED METER
count	98	98	98	98	98
mean	75.9	148.3	28.9	22.9	0.3
std	99.2	134.3	20.2	17.2	0.5
min	0	0	0	0	0
25%	12.6	70.8	17.8	13.0	0.0
50%	29.8	104.5	24.2	18.2	0.0
75%	92.3	187.5	36.2	28.7	1.0
max	403	600	97	90	1

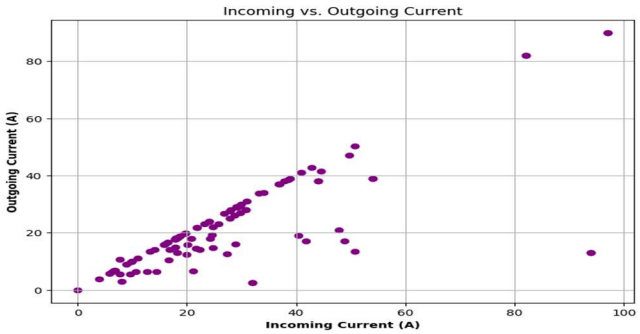

Figure 4: Plot of incoming current vs outgoing current for customer meters

Corresponding author: Oguche Emmanuel Ojochenemi.
ogucheeo@gmail.com
Electrical/Electronic Engineering Department, University of Abuja.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 12(3), SEPTEMBER, 2024
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

Figure 4 shows a scatter plot of **incoming vs. outgoing current** readings at customer meters, highlighting the relationship between these two variables. Most data points align along a positive trend, suggesting a general proportionality between incoming and outgoing currents. However, some outliers exhibit high incoming current with disproportionately low outgoing current, indicating potential energy losses or tampering. This visualization provides a preliminary indicator of irregularities in current flow, which the model aims to detect systematically as part of the theft detection algorithm.

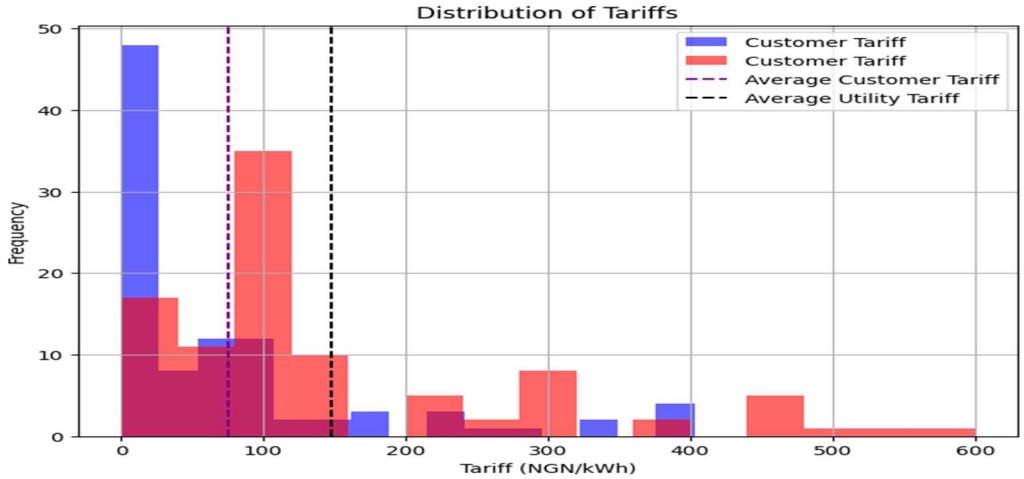

Figure 5: Histogram of customer and utility tariffs

Figure 5 presents a frequency distribution of electricity tariffs for customers and utilities, highlighting the disparities between **customer tariffs** (in blue) and **utility tariffs** (in red). The **average customer tariff** (purple dashed line) is notably lower than the **average utility tariff** (black dashed line), suggesting a common discrepancy where customer-reported tariffs do not align with actual utility rates. The majority of customer tariffs are clustered at the lower end of the scale, while utility tariffs have a wider spread with a significant presence at higher rates. This distribution underscores potential underreporting or manipulation of tariffs, which the model addresses by flagging price deviations as part of the tampering detection process.

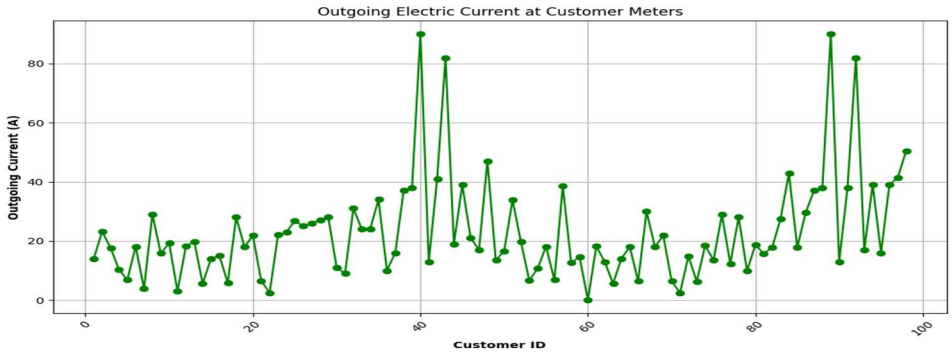

Figure 6: Plot of outgoing power for various customers in the collected data

Corresponding author: Oguche Emmanuel Ojochenemi.
ogucheeo@gmail.com
Electrical/Electronic Engineering Department, University of Abuja.

The line plot in Figure 6 illustrates the **outgoing electric current** across various customer meters, capturing fluctuations in energy consumption patterns. While the majority of customers show relatively stable outgoing current levels, certain customers—particularly those around IDs 40 and 90—display spikes reaching up to 80 A. These sharp increases suggest irregular usage, which could be indicative of tampering or unreported high-load devices. The model identifies such anomalies in outgoing current as part of its tampering detection process, using them as potential indicators of electricity theft.

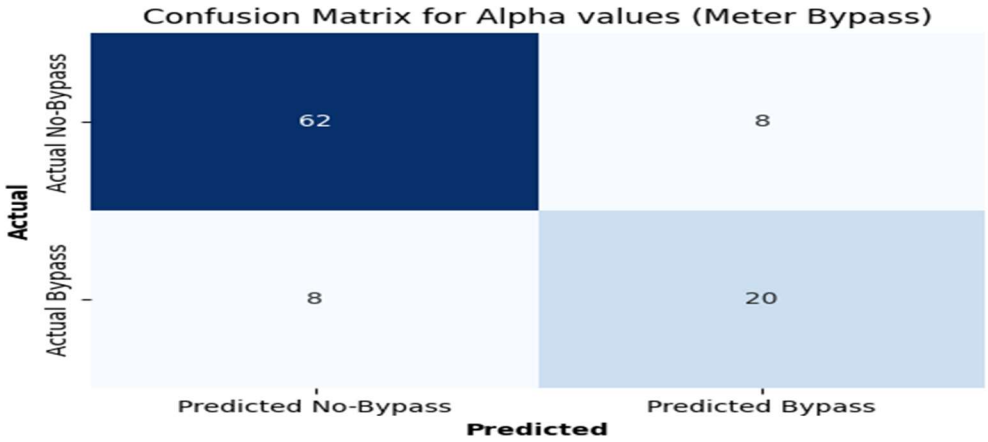

Figure 7: Confusion matrix for Meter Bypass

Figures 7 and 4.6 illustrate the predictive accuracy of the model through confusion matrices for the alpha and zeta metrics, which respectively represent potential meter bypass and tariff tampering detection. In Figure 7, the confusion matrix for the alpha metric shows that the model correctly classified 62 cases of no bypass (true negatives) and 20 cases of bypass (true positives), achieving an accuracy rate of approximately 83.7%. This indicates that the model effectively differentiates between bypassed and non-bypassed meters, though there are 8 false positives and 8 false negatives, showing some margin for improvement in detecting bypass events. With a true positive rate (sensitivity) of 71.4% and a true negative rate (specificity) of 88.6%, the alpha metric performs robustly, balancing sensitivity to bypass events with a relatively low rate of false alarms. These results highlight the model's reliability in identifying bypassed meters, demonstrating the effectiveness of the alpha metric in accurately detecting instances of potential electricity theft.

Similarly, Figure 8 presents the confusion matrix for the zeta metric, which identifies discrepancies in customer tariffs as indicators of tampering. Here, the model correctly classified 45 cases of no tampering (true negatives) and 39 cases of tampering (true positives), achieving an accuracy of 85.7%. This high accuracy underscores the model's capacity to detect tariff manipulation effectively. With only 5 false positives and 9 false negatives, the zeta metric maintains a true positive rate of 81.3% and a true negative rate of 90%, balancing accuracy in flagging actual tampering events while minimizing false positives. Together, the confusion matrices in Figures 4.8 and 4.9 demonstrate the overall prediction accuracy of the model, confirming its capability to accurately identify electricity theft by detecting both meter bypass and tariff tampering. These results validate the model's practical applicability for utility companies seeking to reduce revenue losses due to theft, as it provides a reliable tool for targeting potential cases of tampering in real-world scenarios.

Corresponding author: Oguche Emmanuel Ojochenemi.
✉ *ogucheeo@gmail.com*
Electrical/Electronic Engineering Department, University of Abuja.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 12(3), SEPTEMBER, 2024
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

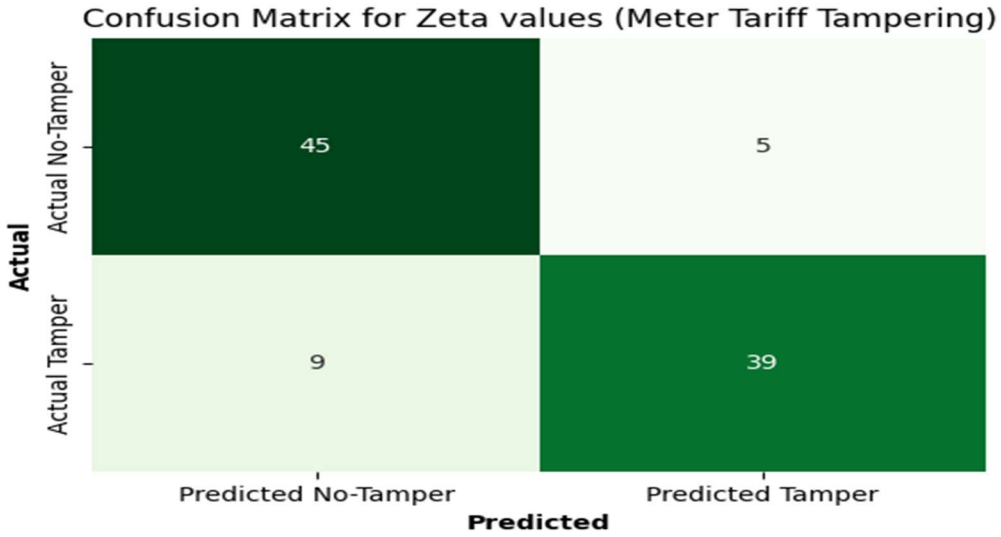

Figure 8: Confusion matrix for Meter Tariff Tempering

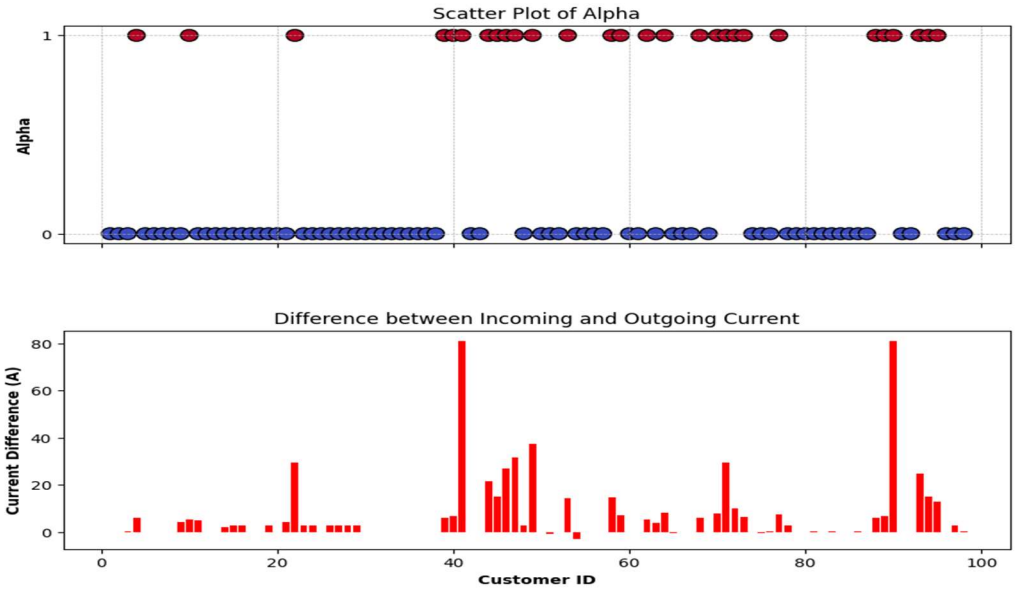

Figure 9: Alpha and power differences for various customers in the collected data

Figure 9 presents' two plots: a scatter plot of the **alpha metric** (top) and a bar plot showing the **difference between incoming and outgoing current** (bottom) across customer meters. In the alpha scatter plot, points labeled as "1" (in red) indicate flagged cases where potential power diversion is detected, while "0" (in blue) represents normal usage. The clustering of "1" values for certain customers suggests instances of suspected tampering. The bottom plot further illustrates current discrepancies, with several large spikes (notably around customer IDs 40 and

Corresponding author: Oguche Emmanuel Ojochenemi.
ogucheeo@gmail.com
Electrical/Electronic Engineering Department, University of Abuja.

90), indicating significant differences between recorded incoming and outgoing currents. These anomalies align with the flagged alpha cases, supporting the detection of tampering. Together, these plots provide visual confirmation of the model's capacity to detect irregularities in power usage patterns.

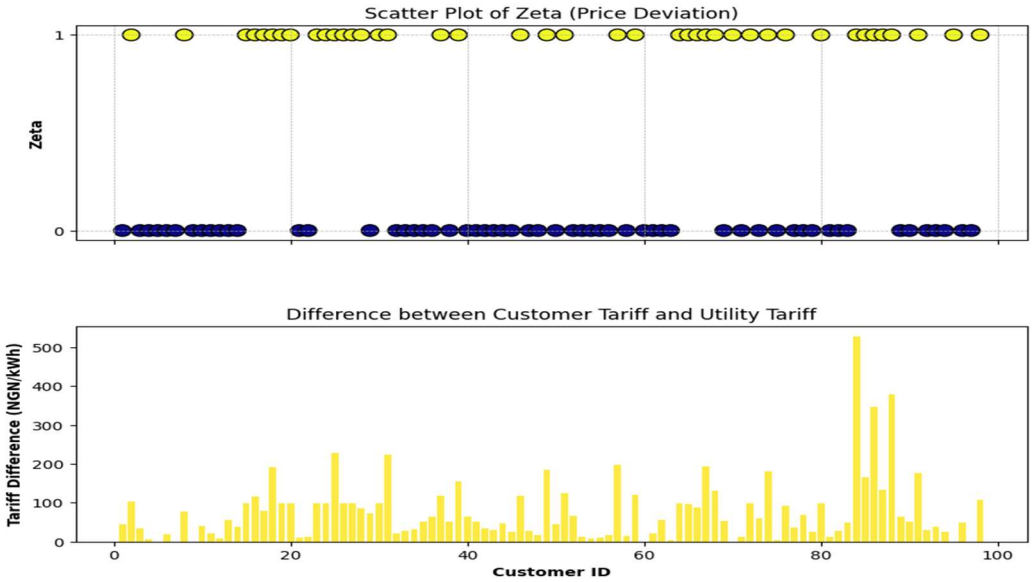

Figure 10: Zeta values and electricity tariff differences for all customers in the collected data

Figure 10 displays two plots: a scatter plot of the **zeta metric** (top) and a bar plot of the **tariff difference** between customer-reported and utility tariffs (bottom) across customer meters. In the zeta plot, points marked as "1" (yellow) represent cases where significant price deviation is detected, while "0" (blue) indicates consistent tariffs. The clustering of "1" values for certain customers highlights cases of suspected tariff tampering. The bottom plot shows the extent of these tariff differences, with notable peaks (especially near customer IDs 80 - 100) indicating substantial disparities between customer and utility tariffs. These variations align with the flagged zeta values, reinforcing the model's ability to identify price discrepancies as potential indicators of tampering.

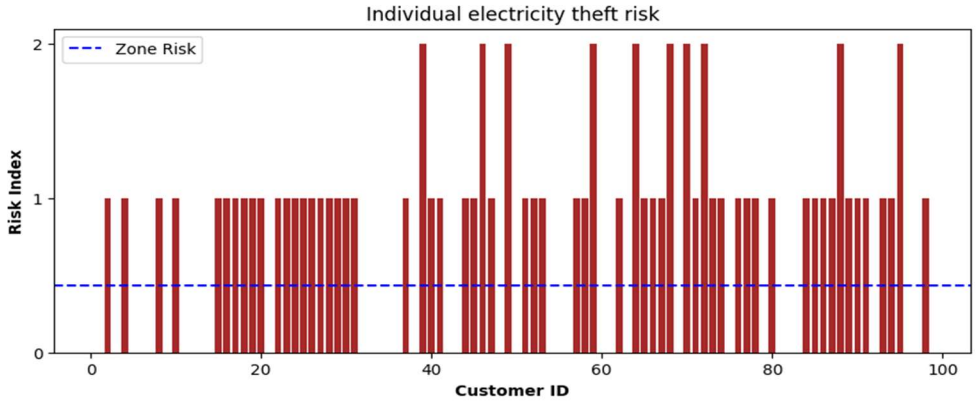

Figure 11: Risk index for customers in the collected data

Corresponding author: Oguche Emmanuel Ojochenemi.
ogucheeo@gmail.com
Electrical/Electronic Engineering Department, University of Abuja.

Figure 11 illustrates the **cumulative electricity theft risk** for each customer, with the individual risk index shown by red bars and the **average zone risk** represented by a blue dashed line. Each customer's risk index reflects the combined impact of the model's metrics (alpha, beta, zeta, and sigma), with values of 2 indicating high-risk customers. Many customers show risk indices exceeding the zone average, suggesting a concentrated risk of tampering in certain segments. This visualization effectively highlights high-risk customers who may require closer monitoring or inspection, thus providing actionable insights for targeted intervention.

CONCLUSION

This study developed a model to detect electricity theft by analyzing smart meter data, focusing on indicators of tampering such as power diversion, time discrepancies, and tariff manipulation. Implemented in Python and validated with both synthetic and real-world data, the model combines multiple metrics to create a flexible, data-driven approach for identifying high-risk customers and zones within a utility network. By integrating advanced metrics and performing sensitivity analyses, the model demonstrates significant predictive accuracy, offering a practical tool for utility companies aiming to reduce non-technical losses. In summary, this model provides a robust and adaptable tool for electricity theft detection, integrating multiple tampering indicators to support informed decision-making in utility management. Future developments could further refine the model by adding additional data sources or exploring machine learning approaches, but as it stands, the current implementation offers a solid foundation for enhancing revenue protection in utility operations.

REFERENCES

[1] N. O. Shokoya and A. K. Raji, 'Electricity theft mitigation in the Nigerian power sector', *International Journal of Engineering & Technology*, vol. 8, no. 4, p. 467, Oct. 2019.
[2] F. M. Dahunsi, A. O. Abdul-Lateef, A. O. Melodi, A. A. Ponnle, O. A. Sarumi, and K. A. Adedeji, 'Smart Grid Systems in Nigeria: Prospects, Issues, Challenges and Way Forward', *ajol.info*, vol. 7, no. 2, 2022.
[3] USAID, 'Power Africa in Nigeria', 2012. https://www.usaid.gov/powerafrica/nigeria (accessed Feb. 02, 2023).
[4] V. N. Ogar, K. A. A. Gamage, and S. Hussain, 'Protection for 330 kV transmission line and recommendation for Nigerian transmission system: a review', *International Journal of Electrical and Computer Engineering*, vol. 12, no. 3, pp. 3320–3334, 2022.
[5] D. Dike, D. O. Dike, U. A. Obiora, E. C. Nwokorie, and B. C. Dike, 'Minimizing household electricity theft in Nigeria using GSM based prepaid meter', *researchgate.net*, no. 1, pp. 59–69, 2015.
[6] O. Olaoluwa 'Electricity theft and power quality in Nigeria', *International Journal of Engineering Research*, vol. 6 no. 6 pp. 1180-1184, June 2017
[7] S. S. Idowu, J. Ibietan, and A. Olukotun, 'Privatization of Power Sector in Nigeria: An Evaluation of Ibadan and Ikeja Electricity Distribution Companies Performance (2005–2018)', *International Journal of Public Administration*, vol. 43, no. 16, pp. 1413–1420, Dec. 2020
[8] O. Oladipo, 'DisCos lose N5m from every N10m worth of energy sold - NERC', 2023.
[9] N. Kambule and N. Nwulu, 'Rationale Part II: A Misdiagnosis of Non-payment and Electricity Theft', *Lecture Notes in Electrical Engineering*, vol. 759, pp. 33–53, 2021.
[10] B. Adetoba, N. Yekini, O. Lawal, and H. Alakiri, 'Enhancing Billing and Minimization of Electricity Theft in the Electrical Power Distribution via ICT, *SMART-SMART-iSTEAMS Conference* Proceedings, pp 95-106, 2018
[11] M. O. Obafemi, E. A. Oluwole, T. E. Omoniyi, P. N. Meduna, and A. S. Alaye, 'Prevalence of electricity theft among households in Lagos State, Nigeria', *Nigerian Journal of Technology*, vol. 40, no. 5, pp. 872–881, 2022.
[12] C. Fidelis, A. David, J. Chukwuemeka, and A. H. Onyinye, 'Controlling Electricity Theft,

Corresponding author: Oguche Emmanuel Ojochenemi.
✉ *ogucheeo@gmail.com*
Electrical/Electronic Engineering Department, University of Abuja.

A Smart Meter Approach: Case Study Nigeria', 2017, Accessed: Jan. 30 2023. [Online]. Available:https://www.researchgate.net/profile/Chukwuebuka-Fidelis-

[13] S. O. Ayanlade, D. Sawyer, and D. T. Sawyer, 'Application of Current Differential Principle in The Detection of Energy Theft in A Gsm-Based Single-Phase Smart Meter', *International Journal of Engineering Technology and Scientific Innovation*, vol. 6 no. 4 pp. 80-90, 2021

[14] A. James, C. Fidelis, A. David, J. Chukwuemeka, and A. H. Onyinye, 'Abating Electrical Power Theft in Nigeria Using Smart Meters and Data Analysis', 2019, Accessed: Jan. 30, 2023. [Online]. Available: https://www.researchgate.net/profile/Chukwuebuka-Fidelis-

[15] S. Solaimalai, S., Semwal P., Palit, S., and Indulkar, 'Smart Metering in Smart Grid', *International Journal of Engineering Advanced Technology*, vol. 8, no. 4, pp. 1021–1027, 2019.

[16] K. I. Saeed MS, Mustafa MW, Hamadneh NN, Alshammari NA, Sheikh UU, Jumani TA, Khalid SB, 'Detection of non-technical losses in power utilities—A comprehensive systematic review.', *Energies (Basel)*, vol. 13, no. 18, p. 4727, 2020.

[17] N. T Makanjuola, O. O Shoewu, L. A. Akinyemi, and O.D. Ogunsanya, 'Research, and undefined 2019, 'Investigation on Smart Meters and Revenue Generated for a Year Using Eko Electricity Distribution Company of Nigeria as Case Study', *Data Research*, vol. 3, pp. 2617–4537, 2019

[18] B. Adebanji, A. Ojo, T. Fasina, S. Adeleye, and J. Abere, 'Integration of renewable energy with smart grid application into the Nigeria's power network: Issues, challenges and Opportunities', *European Journal of Engineering and Technology Research,* vol. 7 no. 3 pp 18-23, 2022.

[19] K. Alao, K. Jimoh, and A.J. Obadiora, 'Evaluation of Customer Education and Satisfaction of Prepaid Meter Usage in Nigeria Electricity Distribution Company'. *Journal of Digital Learning and Education,* vol. 4, no. 1 p. 775, 2022, doi: 10.35629/5252-0409775781.

Corresponding author: Oguche Emmanuel Ojochenemi.
✉ *ogucheeo@gmail.com*
Electrical/Electronic Engineering Department, University of Abuja.