:: IJEEIT ::
(International Journal of Electrical Engineering and Information Technology)
Volume 07 Number 02 September 2024

ISSN : 2615-2096 (ONLINE)
ISSN : 2615-2088 (PRINTED)

An Integrated Power System Machine Learning Model for Detecting Smart Meter Frauds in Distribution System: Case study of PHED Market

Biobele A. Wokoma
Department of Electrical and Electronics Engineering, Rivers State University, Port Harcourt, Rivers State, Nigeria.
biobele.wokoma@ust.edu.ng

Elijah O. Olubiyo
Department of Electrical Engineering, University of Nigeria, Nsukka, Enugu State, Nigeria.
elijah.olubiyo.162135@unn.edu.ng

Maxwell O. Nwoku
Department of Computer Engineering, Rivers State University, Port Harcourt, Rivers State, Nigeria.
nwoku.maxwell@ust.edu.ng

Ibitroko B. A. Wokoma
Department of Centralized System Operation and Dispatch, Port-Harcourt Electricity Distribution Company, Port Harcourt, Rivers State, Nigeria.
ibitroko.wokoma@phedc.com.ng

ABSTRACT
Smart meter billing systems represents the modern state-of-the art in pre-paid billing as the move from estimated bills within the Nigerian state now becomes a priority to circumvent the heavy fraud situation. However, the detection of fraud in real-time smart meter systems presents an opportunity for more dynamic approaches to be employed due to the unique nature of this billing system. In this paper, an emerging auditory inspired neural technique that supports continual learning and adaptive processing of temporal streaming data states is proposed for the detection of smart meter fraud. The technique is integrated in a simulated power system program and applied to the detection of frauds in two feeder units of a Port-Harcourt Electricity Distribution (PHED) business district. Simulation results showed that the proposed approach is a potential candidate for detecting fraud in smart meter billing systems with minimal mean absolute percentage errors.

Keywords: Billing, Fraud, Neural Networks, Power Distribution, Smart Meter.

1. INTRODUCTION

The issue of frauds in the Nigerian power sector is not novel due to the sorry state of the industry as it borders on operational management, human resource re-branding, State-of-the-Nation amongst other issues. Just as in the financial economy, there can be fraud in the power economy as a result. One of the primary indicators of fraud in the power sector is the usual billing error due to such issues as large data handling, repetitive manual calculations and/or intentional doctoring by PHED staff. There is also at the consumer end, the most likely tampering of the power side on installed meters leading to unusual billing errors or absence of billing entirely.

Thus, the power system distribution operators are faced with the dilemma of incessant power and monetary losses due to such frauds while trying to deliver power at expected quantitative levels and quality. The power losses which lead to monetary losses constitute non-technical losses (NTL) (Sahoo et al, 2015).

These challenges make smart meters particularly useful but the added challenge of tampering and possible breaches by staff or consumer still applies but at somewhat advanced levels.

Current research in the field has shown the advantages of using computerized billing approaches to salvage smart meter frauds. Computerized billing is preferable to manual billing due to the ease of handling very large volumes of data, repetitive operations, complicated computations, consistent accuracy, fast response processing, fraud detection, and minimization of fraud (Abdulwahab, 2009).

In this research paper, a dynamic programming approach based on an emerging neural approach called the Neuronal Auditory Machine Intelligence (NeuroAMI) is proposed for the detection of smart meter frauds in distribution power systems.

Energy meters installed at the consumer terminals provides the basis for the billing of the energy consumed. Besides this, the meter reading also help in the computation of energy loss in the distribution network (Thakur et al., 2002). Customers are expected to pay the bill as metered for energy the used after a given period. Challenges however arise because the payment is billed after usage and the company has no means to recover even when the bills are not settled. This is the post-pay method which has been noted to be no longer realistic as it does not support revenue collection efficiency. Thus, smart metering systems are typical in modern infrastructures.

The smart metering system is one in which the meter is preloaded with electric energy units available for service. The meters have been programmed to cut off supply after the loaded energy units has been exhausted. As the units get depleted by usage, an alert is sent to consumers at pre-set limits to recharge or load more credit units. If the consumer fails to adhere to the prompt, supply will eventually be remotely disconnected as soon as the payment is exhausted.

Consumers are also automatically re-connected as soon as more energy units are loaded. Ofonyelu (2014) observed that number of evidences suggest that electricity billing in Nigeria is asymmetric before the introduction of pre-pay smart meters. The largest occurrence of asymmetry in electricity billing occurs for consumers who were not metered. It occurs because ownership of meter gives room for consumers to monitor their consumption and know the amount of energy actually consumed. Being metered gives the consumer opportunity to be able to calculate own bill, having known the amount of energy consumed. As a result, metering essentially helps to reduce the tendencies for asymmetry.

Amadi (2013) also observed that the issuance of estimated bills by the electricity distribution companies (discos) gives room to cheating the consumers. Estimated billing system is said to be analogous to fraud where consumers are made to pay far above what they consume monthly (Fagbohun & Femi-Jemilohun, 2017). However, to the consumers, it is two pronged – while the high energy users may be comfortable to pay the allocated flat rates no matter their actual energy consumption, the low end users feels cheated to pay more for the services received. The end result is that many customers are not ready to pay for the energy consumed thereby the company losses a lot of income from these customers.

Also, it was the opinion of research by Ogun and Ofonyelu (Ogun & Ofonyelu, 2013) that metering all electricity consumers would assist the customer to effectively monitor their electricity usage, as well as enable the Distribution Companies (DISCOS) determines their revenue thereby

ISSN : 2615-2096 (ONLINE)
ISSN : 2615-2088 (PRINTED)

driving for its collection. The prepaid metering platform was aimed at addressing the asymmetries from both the sides of the consumers and the utility company.

Prepaid smart meters have the advantage of being able to automatically cutting off supply to consumers at the exhaust and/or expiry of paid electricity energy units without physical disconnection from the grid as is usually the case with post-paid and estimated billing systems. It also eliminates the frequency of unpaid bills and lowers overhead costs because the meter readers are eliminated and their services may be utilised in other assignments. But it does not entirely prevent smart meter frauds.

Recent research directions in smart meter fraud detection using conventional supervised Artificial Neural Network (ANN) models assume the meter data to be a static representation of real-time processes in addition to issues such as often big-data and needless feature engineering requirement (Ford et al., 2014; Ullah et al., 2021). Even their Deep Learning (DL) alternatives such as applied in (Badr et al., 2021) are faced with the problem of over-parameterization and also the big-data requirement to learn on simple things. As a result, the temporal properties and intermittent small data availability that occur in smart metering systems are not accounted for in these models. This may be attributed to the inherent nature of the employed ANN models being of static processing ability and large number of unnecessary layers needed for learning the world.

Thus, there is need to consider other ANN models that support temporal processing which this research seeks to investigate.

2. RESEARCH METHOD

The materials employed in this study comprise of the power station distribution data for the Obiwali and Airport feeders obtained from the Rumuodomaya business unit of the Port-Harcourt Electricity Distribution (PHED) company of Nigeria. The nature of the considered data for fraud detection is as presented in Table 1.

Table 1: Data for Smart Meter Fraud Studies (Rumuodomaya Business Unit – PHED)

Parameter	Data Type
Meter Condition	Symbolic (Bad or Good)
Average Monthly Billing	Numeric (Real-Type)

Considering the data attributes in Table 1, it is expected that once the account is billed, the meter is believed to be in a good working state. If the meter is bad then no billing is expected. These indications can be determined from the signal status function available in many smart meters.

The operation of smart meter with respect to billing and meter state can be formulated mathematically as:

$$SM_{state} = \begin{cases} k_i, & if\ M_{cond} = good \\ k_j, & if\ M_{cond} = bad \\ k_k, & if\ M_{cond} = disconnectanomaly \end{cases} \tag{1}$$

ISSN : 2615-2096 (ONLINE)
ISSN : 2615-2088 (PRINTED)

SM_{state} : state of Smart Meter (SM) - whether meter is good, bad or there is a disconnect or suspected anomaly

M_{cond} : condition of smart meter as at when a request for billing status is made

k_i, k_j, k_k : the automatically encoded classes corresponding to good, bad and disconnect anomaly states

It is important to emphasize here that when the smart meter power signal status state is active, a remote request will be made to the PHED customer server database to retrieve data.

2.1. Methods

The proposed method is based on dynamic programming model that learn to adjust adaptively its learning parameters during prediction of anomalous smart meter readings. Just as in most simulation studies it follows from a set of assumptions for the identification of frauds in smart meter readings and for a given PHED business district. These assumptions are:

- Smart Meter (SM) readings for a set of PHED customers are presented continually in sequentially streaming manner with the state of the meter (Good, Bad or anomalous) followed by its corresponding billing state (Charged or Non-Charged).
- A fraud state is determined by a Disconnected (DC) meter that may be assigned a Charged or Non-Charged billing state.
- There are 3 possible SM detection states – a bad state, good state or disconnect (DC) (anomalous) state.
- A set of 3 repeated DC signals indicate a most likely fraudulent act within the studied business district.
- Smart meters are equipped with the necessary sensors to detect faulty (bad or non-functional) and fraudulent (possible disconnect) states using remote messaging facilities to PHED business district(s).

2.1.1. System Methodology

In order to identify SM frauds in power systems using modern computerized approaches, it is necessary that an integrated learning dynamic programming approach be adopted. The proposed integrated power machine learning model systems view for detecting smart meter frauds is as shown in Figure 1.

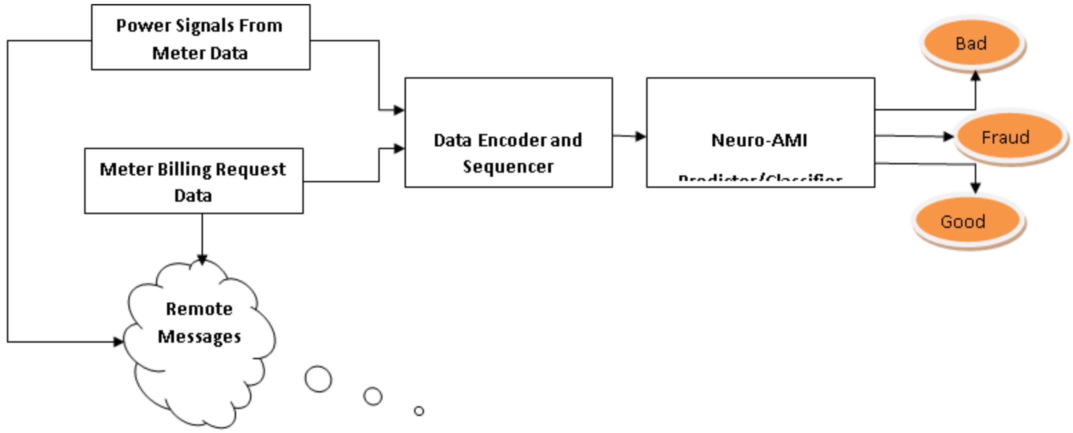

Figure 1: Integrated Power Machine Learning Model

:: IJEEIT ::
(International Journal of Electrical Engineering and Information Technology)
Volume 07 Number 02 September 2024

ISSN : 2615-2096 (ONLINE)
ISSN : 2615-2088 (PRINTED)

As can be clearly seen, smart meter data is obtained from power signals (status indicators) denoting state of meter and the billing state. This is followed by specific encoding and sequencing then the NeuroAMI classifies the data into good and bad states.

2.1.2. NeuroAMI Classifier

This research study considers NeuroAMI architecture (see Figure 2) as a classifier for smart-meter fraud. It includes logical and functional circuitry for implementing and auditory-inspired neural processing approach (Osegi & Anireh, 2020; Osegi, 2023).

The NeuroAMI ANN specifically implements two fundamental concepts that are based on the Change Detection (CD) and Model Adjustment (MA) principles. It also incorporates some very desirable properties of neural systems such as temporal adaptation, sparse connectivity operation, not overfitting on training data, in addition to a clear-cut deterministic learning process. Further details on this technique can be found in (Osegi, 2023).

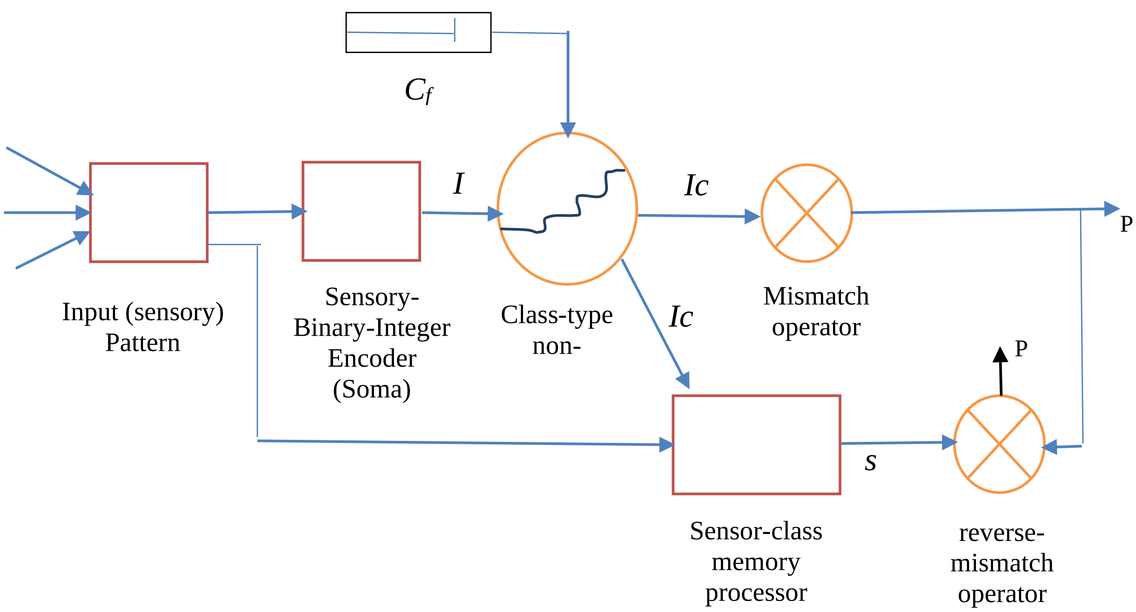

Figure 2: The Updated NeuroAMI Architecture (Osegi, 2023)

3. RESULT AND DISCUSSION

The results are reported in terms of the encoded class states, actual and predicted values and the Mean Absolute Percentage Error (MAPE) considering a limited dataset (26 data samples for the Obiwali feeder and 51 data samples for Airport feeder) with 35% of each dataset used for training and remaining 65% for testing. The parameters for the NeuroAMI are as provided in Table 2.

Table 2: NeuroAMI Parameters

Parameter	Value
Deviant Adjust	2
Population of neurons	1000
Class level	3

ISSN : 2615-2096 (ONLINE)
ISSN : 2615-2088 (PRINTED)

3.1. Results for Obiwali Feeder

The encoded pattern class states as found by the proposed NeuroAMI ANN fraud detector system, are as shown in Table 3.

Table 3: Encoded Pattern Classes (Obiwali Feeder)

Found Pattern State	Class
'GOOD	1
'BAD	2
'DC	3

As can be seen from Table 3, the number of found patterns cofirm to the tri-state representation as defined in the set of assumptions (see Section 3, sub-section 3.1). Thus, the 3-class problem is fully represented by the NeuroAMI ANN for the Obiwali feeder data.

In Figures 3 and 4 are shown the training and test prediction vs. actual values respectively. Also shown in Figure 5 is the MAPE for the entire continual learning process.

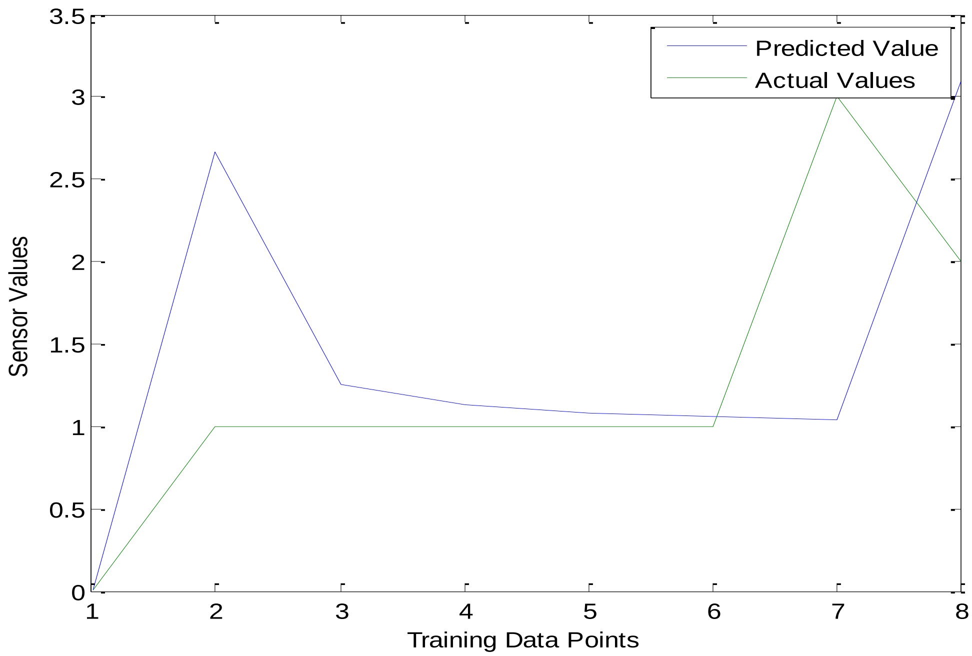

Figure 3: Training Prediction vs. Actual results (Obiwali Feeder)

ISSN : 2615-2096 (ONLINE)
ISSN : 2615-2088 (PRINTED)

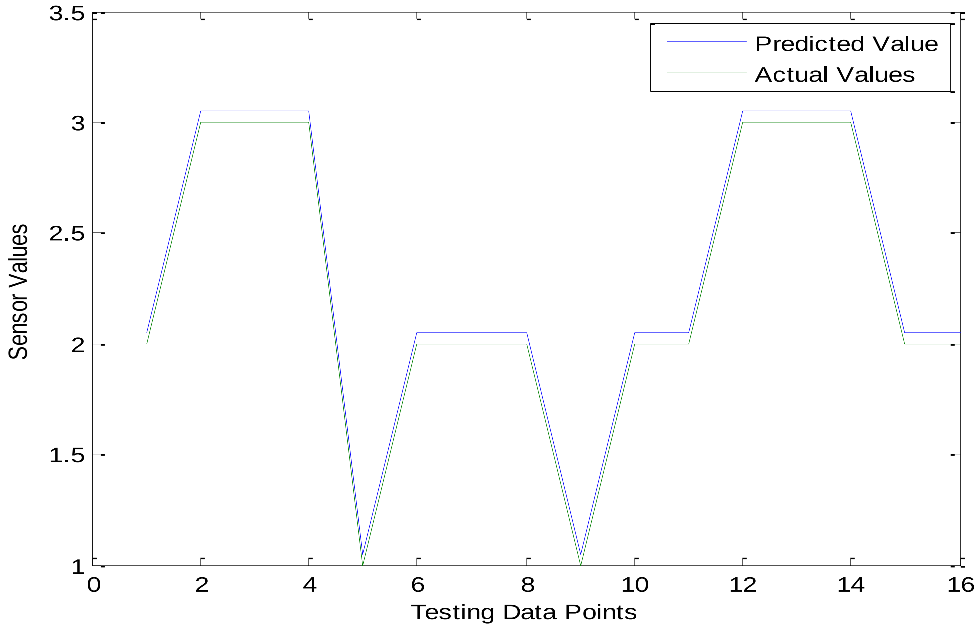

Figure 3: Test Prediction vs. Actual results (Obiwali Feeder)

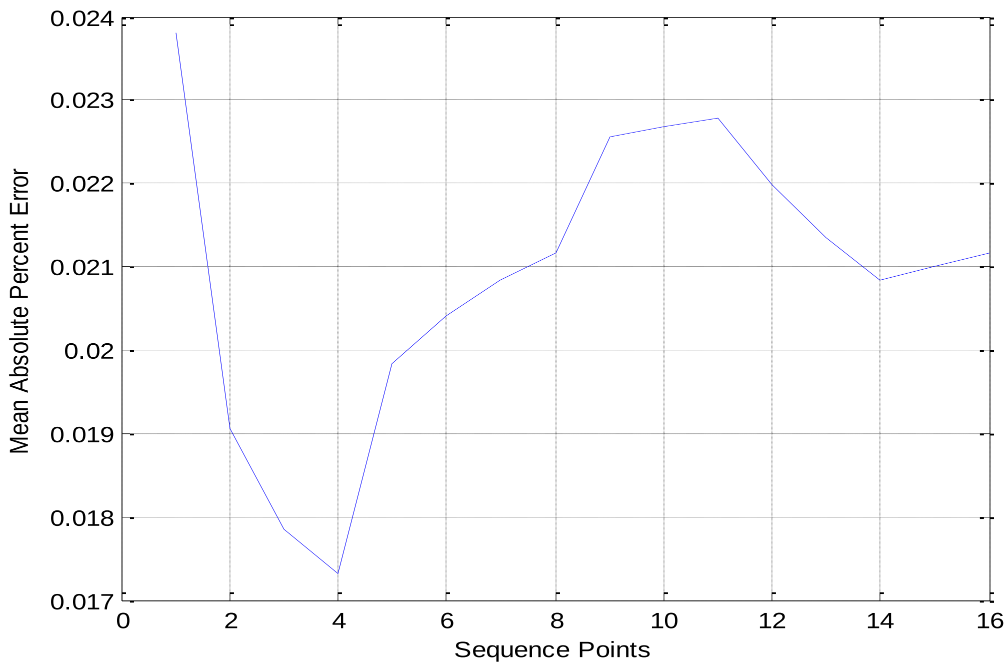

Figure 4: Continual learning MAPE results (Obiwali Feeder)

As can be seen from training performance (Figure 3), the class prediction deviates widely from actual values between the first and last 3 data points (between data points 1-3 and 6-8). However, in-between data points 3 and 6, the deviation is quite minimal. Also Figure 3 shows a

:: IJEEIT ::
(International Journal of Electrical Engineering and Information Technology)
Volume 07 Number 02 September 2024

ISSN : 2615-2096 (ONLINE)
ISSN : 2615-2088 (PRINTED)

tendency to predict the fraud state (class 3) from data points 2 – 4, and 12 – 14 implying that the SMs used in this district are more likely compromised.

From Figure 4, the test performance is approximately close to the expected class value. This great improvement can be inferred from the MAPE response plot (see Figure 4) showing a graded fast decrease in error as the learning data points increases from data points 1 to 4, a staggered rise from points 4 to about 9 and then a staggered fall from points 9 to 14.

3.2. Results for Airport Feeder

As in the Obiwali feeder, the encoded pattern class states found by NeuroAMI ANN is as shown in Table 4.

Table 4: Encoded Pattern Classes (Airport Feeder)

Found Pattern State	Class
[]	
'DC	2
'GOOD	3

As can be seen from Table 3, the number of found patterns is only two with an empty class at the expected first entry. This implies that the NeuroAMI ANN system viewed the data mining process as a bi-state (2-state) learning problem. Thus, the 3-class problem is partially represented by the NeuroAMI ANN for the Airport feeder data.

The training prediction vs. actual value response plots, test prediction vs. actual value response plots and the MAPE responses for the entire continual learning process are as shown in Figures 5, 6 and 7 respectively.

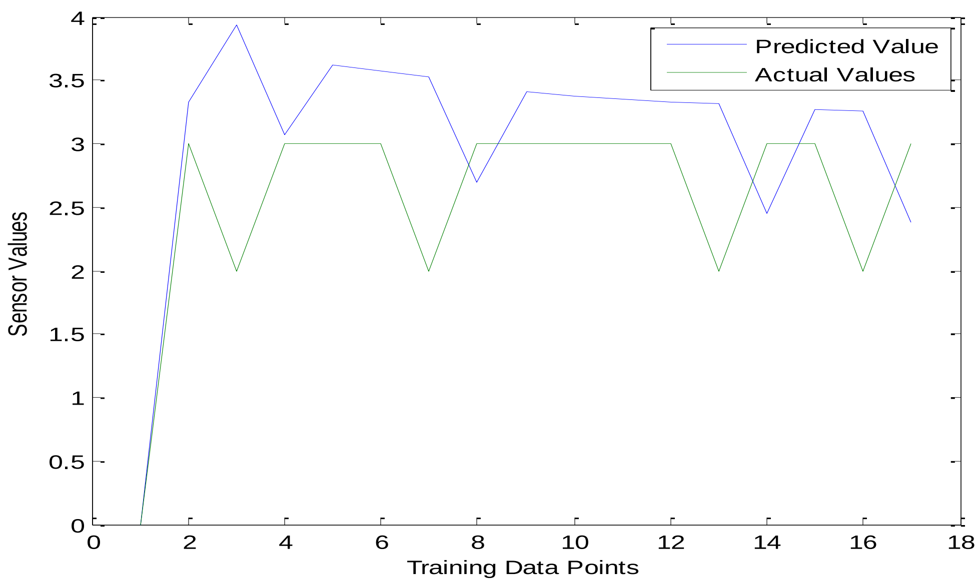

Figure 5: Training Prediction vs. Actual results (Airport Feeder)

ISSN : 2615-2096 (ONLINE)
ISSN : 2615-2088 (PRINTED)

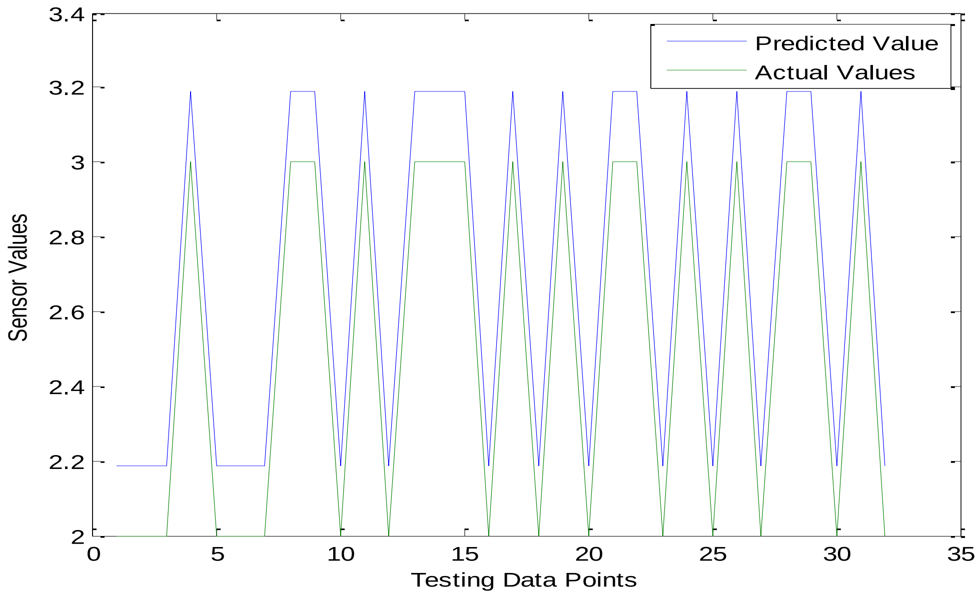

Figure 6: Test Prediction vs. Actual results (Airport Feeder)

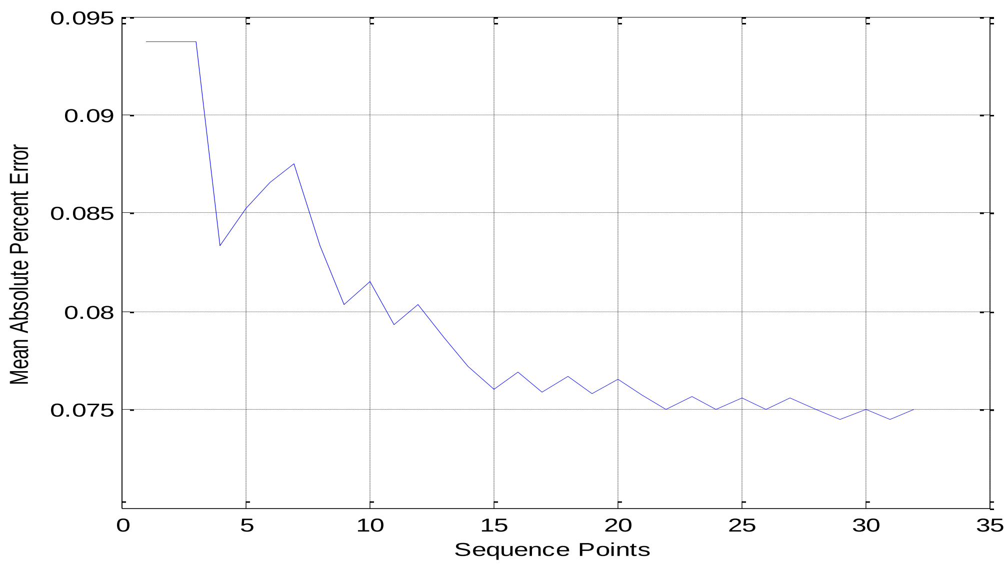

Figure 7: Continual learning MAPE results (Airport Feeder)

As can be seen from training performance (Figure 5), the class prediction there is very slight deviations between prediction and actual values for the first 3 data points but the deviations increase marginally and then fluctuates within the sensor class boundaries of between 2 and 4 with an interesting line-following characteristic for the remaining data points.

The test performance (Figure 6) shows that within the limits of experimental machine intelligence error, the actual and prediction values are very close with a high tendency toward the GOOD state. This is clearly evident in the graded fall in MAPE error shows (see Figure 7). It can

ISSN : 2615-2096 (ONLINE)
ISSN : 2615-2088 (PRINTED)

further be explained by the regular data pattern as the number of GOOD states is far higher than that of the FRAUD or BAD state for the Airport feeder when compared to the Obiwali feeder.

4. CONCLUSIONS

This research paper has proposed an integrated power systems machine learning model useful for detecting smart meter (SM) frauds. The studies identified the benefits of continual learning neural model approaches as opposed to static learning models. The application on two feeder datasets from PHED business district revealed the potentials of the proposed solution particularly as it pertains to the automatic detection and prediction of likely anomalous or fraudulent patterns in real-time.

Future research will consider the application on real-time systems including embedded systems hardware integration and cloud computing techniques in the presence of possible cyber attacks.

Acknowledgement

The SurePay Foundations Group is acknowledged for programming services.

REFERENCES

Abdulwahab, L. (2009). *An Assessment of Billing Electricity Consumers via Analogue Meters in Kano, Nigeria, Kano Electricity Distribution Plc*. Bayero Journal of Pure and Applied Sciences, (2)1 pp 27-33, June 2009

Amadi, S., 2013. *FG cautions new power firms owners against crazy bills.* Available from http://www.nigeriancurrent.com/business-news/item/4915-fg-cautions-new-power-firms-ownersagainst-crazy-bills.html [Accessed 15/04/2018].

Badr, M. M., Ibrahem, M. I., Kholidy, H. A., Fouda, M. M., & Ismail, M. (2023). Review of the data-driven methods for electricity fraud detection in smart metering systems. Energies, 16(6), 2852.

Fagbohun, O., & Femi-Jemilohun, O. (2017). Prepaid metering empowerment for reliable billing and energy management of electricity consumers in Nigeria. *Journal of Scientific Research and Reports*, *17*(2), 1-13.

Ford, V., Siraj, A., & Eberle, W. (2014, December). Smart grid energy fraud detection using artificial neural networks. In 2014 IEEE symposium on computational intelligence applications in smart grid (CIASG) (pp. 1-6). IEEE.

Ofonyelu, C. C. (2014). Metered and unmetered billing: How asymmetric are the Phcn Bills?. *Journal of Social Economics Research*, *1*(5), 97-107.

Ogun, O. and. Ofonyelu, C.C. (2013). *Asymmetric Information Problems in the Nigerian Banking Industry: Any scope for institutional reforms?* Paper Presented at the 54th Annual Conference of the Nigerian Economic Society, between September 17-19, 2013 at Sheraton Hotel and Towers, Abuja.

Osegi, E. N., & Anireh, V. (2020). AMI: an auditory machine intelligence algorithm for predicting sensory-like data. *Computer Science*, *5*(2), 71-89.

Osegi, E. N., Jagun, Z. O., Chujor, C. C., Anireh, V. I., Wokoma, B. A., & Ojuka, O. (2023). An evolutionary programming technique for evaluating the effect of ambient conditions on the power output of open cycle gas turbine plants-A case study of Afam GT13E2 gas turbine. *Applied Energy*, *349*, 121661.

Sahoo, S., Nikovski, D., Muso, T., & Tsuru, K. (2015). Electricity theft detection using smart meter data. *2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 1-5.

ISSN : 2615-2096 (ONLINE)
ISSN : 2615-2088 (PRINTED)

Thakur, T., Agnihotri, G., & Ahirwar, C. (2002). Modernization of Metering, Billing and Collection System, the Customer Relationship Management. In *National Power Systems Conference, NPSC* (pp. 27-29).

Ullah, A., Javaid, N., Yahaya, A. S., Sultana, T., Al-Zahrani, F. A., & Zaman, F. (2021). A hybrid deep neural network for electricity theft detection using intelligent antenna-based smart meters. Wireless Communications and Mobile Computing, 2021, 1-19.