



DETECTION OF ELECTRICITY METER BYPASS IN NIGERIA USING MACHINE LEARNING

¹Onyia Jerry O., ²Ugwu Edith A., ³Asogwa Tochukwu C., ⁴Anameje Chinwe A.

^{1,2,3,4}Department of Computer Science

^{1,2,3}Enugu State University of Science and Technology, Enugu State; ⁴Federal Polytechnic, Oko, Anambara, State, Nigeria

¹jerryobiajulu3@gmail.com; ²edith.ugwu@esut.edu.ng, ³tochukwu.asogwa@esut.edu.ng

⁴chinweanameje16@gmail.com

Abstract

This study focused on the detection of electricity meter bypass in Nigeria using machine learning algorithms. The aim was to develop an intelligent model with the capacity to detect potential customers involved in energy theft through meter bypass. To achieve this, data as collected from the Enugu Electricity Distribution Company (EEDC), considering customer meter recharge information and then transformed to train Support Vector Machine (SVM) and Artificial Neural Network (ANN) algorithms and generate models for the classification of energy theft. The evaluation of the models considered metrics such as accuracy, True Positive Rate (TPR), and False Negative Rate (FNR). The results demonstrated that both SVM and ANN models achieved high accuracy and TPR, with the SVM model having an accuracy of 93.9% and TPR of 100%, and the ANN model achieving 100% accuracy and TPR of 100%. Comparative analyses with existing models showed that the proposed SVM and ANN models outperformed previous methods in terms of accuracy and TPR. The limitation of the study is that it still requires other investigation to prove that a customer involved in energy theft, while the new system facilitated the process.

Keywords: Artificial intelligence, TPR, FNR, ANN, electricity meter bypass, SVM, EEDC

1. Introduction

In recent years, electric power systems have been going through significant digital growth thanks to the utilization of techniques previously used in Information and Communication Technologies (ICT) (Czechowski & Kosek, 2016). Remote management and monitoring of smart grids is increasingly often encountered in virtually every part of power grid infrastructures, from grid and operator system management centers to installations with devices electric power meters (Bush, 2014). The importance of metering in the electricity sector value chain cannot be over-emphasized. It has been described as the cashbox of the electric power sector industry because the revenue generation process in the value chain starts from the meters installed at locations such as homes, offices, and industries to determine for appropriate costing, the amount of the transmitted and distributed electricity consumed at the various locations. Hence, electric meters are usually installed at customers' premises to measure electric energy delivered to customers for

billing purposes. They are calibrated in billing units which operate by continuously measuring the instantaneous voltage (volts) and current (amperes) which is accessed by the different distribution companies (DisCos) to give energy used (in joules, kilowatt-hours, etc.) (Aladeitan and Joan, 2020).

According to Usman (2013), a study showed that customers were dissatisfied with the services of Distribution Companies (DisCos) due to their dissatisfaction with the use of analog meters and estimated billing. This and some other factors like poverty, which is one of the main factors affecting consumers today has led many of them to engage in electricity energy theft by bypassing their meters, which resulted in them consuming electricity that they didn't pay for and also was not recorded by their meters thereby paying less and consuming more. These culprits achieve this form of electricity theft by directly connecting armored cables from the main power grid to the building or facility, often during the night hours to avoid being caught by officials of distribution companies or members of task forces dedicated to combating electricity meter bypass (The Sun, 2022). According to Nkemneme (2020), another factor for this trend is that customers do not consider electricity theft to be unethical; rather, they believe that it is their fundamental social right to have access to electricity without paying for it.

In Nigeria, this issue of electricity meter bypass has become widespread, with observations indicating that approximately 80 out of 100 residents in a particular area engage in this form of theft. When incidents of meter bypass are reported, utility companies dispatch investigation teams to monitor the affected areas. Electricity meter bypass became too much of a burden on DisCos which resulted in the formation of a special task force to this effect which most times were accompanied by some law enforcement personnel to help track down those that carried out this form of electricity theft, these teams typically arrive during the day, unaware that bypass activities predominantly occur at night or on weekends. In most cases, corruption played a role, as members of the task force were sometimes bribed not to report a defaulter who had been caught, or in some other cases, the defaulter might be related to a member of the task force, so they would return to the office and deliver false reports. The losses incurred by these distribution companies cannot be ignored, as they not only lose money from the electricity that is consumed and not accounted for, but also from the human resources that are members of the task force, as they are paid for a job that they often do not deliver. The use of human resources by these distribution companies to help track down the bypassing of electricity meters has been far from adequate. To address this challenge, the research proposes the utilization of AI algorithms and advanced data analytics techniques to develop an intelligent model capable of monitoring electricity consumption patterns, detecting anomalies, and identifying instances of tampering or bypassing. By leveraging these technologies, the research aims to enhance meter bypass detection, reduce revenue losses, and improve operational efficiency for utility companies

2. LITERATURE REVIEW

Bohani, et. al., (2021) performed a comprehensive analysis of supervised learning techniques for electricity theft detection. Several supervised learning methods such as Decision Tree (DT), Artificial Neural Network (ANN), Deep Artificial Neural Network (DANN), and AdaBoost were

presented and compared based on different evaluation metrics; predictive accuracy, recall, precision, Area Under Receiver Operating Characteristics (ROC) Curve (AUC), and F1-score and their performances were also analyzed. After which it was recorded that ANN showed the highest average of accuracy with 92.54%, followed by DANN (92.31%), Ada-Boost (91.75%), and DT (91.39%). After evaluation on AUC; DT, ANN, DANN, and AdaBoost had the highest score with the values of 0.5149, 0.7029, 0.7130, and 0.5418. The F1-score also yielded the following result with 6.10%, 49.50%, 52.44%, and 15.45%, respectively. After the precision evaluation was used, ANN, DANN, and AdaBoost, performed the best precision with 79.03%, 65.71%, and 63.64%, respectively. DT however showed 53.97% precision. As for recall, DANN outperformed other methods with 40.94%, followed by ANN (35.49%), AdaBoost (7.57%), and DT (2.87%), ANN and DANN produced the highest recall at a 60/40 ratio with 50.71% and 61.03%, respectively. Despite the success achieved by this model, there is still room for improvement in the F1-score as the Deep Artificial Neural Network (DANN) produced the best result at 52.44% which is fair but leaves room for great improvement.

Ullah, et. al., (2021) researched the detection of electricity theft. A hybrid model was presented in the study, which combined convolutional neural network, particle swarm optimization, and gated recurrent unit, this brought about the term Convolutional Neural Network-particle swarm optimization-Gated Recurrent Unit model (CNN-GRU-PSO). The major aim of the model was to accurately detect electricity theft and also to overcome the issues encountered in other existing models like; Ensemble Bagged Tree (EBT) for detecting Non-Technical Losses (NTLs) in power grids, a hybrid approach based on the Gaussian Mixture Model (GMM) and Long Short Term Memory (LSTM), Maximal Overlap Discrete Wavelet Packet Transform (MODWPT) based model for feature extraction and Random Undersampling Boosting (RUSBoost) technique to detect NTLs in the power grids. The issues from these models include over-fitting and the inability of those models to handle imbalanced data. The proposed model made use of electricity consumption data from smart meters obtained from the state grid corporation of China. It was however deduced from the result of the study that the proposed Hybrid Deep Neural Network (HDNN) model was more efficient in handling imbalanced issues and performing electricity theft detection. However, the dataset for the model contained real-time data with missing values and outliers which led to a training accuracy result of 81% which is good. However, more improvement can be made to get a higher accuracy result. Petrlík, et. al., (2022) researched electricity theft detection. The research aimed to recommend the best prediction model using Machine learning in electrical energy theft. The dataset was based on the electricity consumption data of 42372 consumers published in the State Grid Corporation of China. The method used in the research was data imputation, data balancing (oversampling and under-sampling), and feature extraction to improve energy theft detection. Five machine learning models were tested, these include the Support Vector Machines model (SVM), Random Forest (RF), K-Nearest Neighbors (KNN), Naive Bayes (NB), and Logistic Regression (LR). After evaluation, the accuracy indicator for the models was as follows; 81%, 80%, 79%, 68%, and 69%, respectively. From the results of the study, it was concluded that the SVM model had the best performance, with an

accuracy of 81%. Despite the high accuracy result of this model, there is still room for improvement.

Hussain, et. al. (2022) presented a study on electric theft detection in advanced metering infrastructure. Furthermore, a top-to-bottom execution of a supervised machine learning-based electric theft detection framework was presented using a Jaya-optimized combined Kernel and Tree Boosting (KTBoost) classifier. This implored the intelligence of the Extreme Gradient(XGBoost) algorithm to estimate the missing values in the acquired dataset during the data pre-processing phase. Also, an oversampling algorithm based on the Robust-SMOTE technique was utilized to tackle the issue of unbalanced data class distribution issue which resulted from the estimation carried out by the Boosting (XGBoost). The ensemble machine learning-based classifier KTBoost, with Jaya algorithm, and optimized hyper-parameters, is used to effectively classify the consumers into Honest and Fraudulent. The outcome of this study reveals that the proposed electric theft detection method achieves the highest accuracy (93.38%), precision (95%), and recall (93.18%) among all the studied methods. After evaluation, the proposed machine learning algorithm in this study obtained an accuracy score of 93.8% which is high but improvements can still be made. Saha, et. al., (2020) presented a study based on the detection of abnormalities and electricity theft using machine learning analytics. The study showed that 80% of energy losses were brought about by non-technical losses which is hard to identify and evaluate this made it in need of more advanced technology. Linear regression method which predicts continuous numerical values based on given input data was used for anomaly detection in this study. The method presented, improved detection accuracy, sensitivity, and reduced magnitude of data required. However, other aspects such as high accuracy of predicting could not be maintained in this method as that of other sophisticated algorithms.

Aniedu, et. al., (2022) presented a machine learning-based system for energy loss detection and monitoring in advanced metering infrastructure. The study showed that Non-Technical Losses (NLT) occurred because of theft and other fraudulent activities surrounding the illegal consumption of energy. It was however stated in the study that although Advanced Metering Infrastructure (AMI) incorporating smart meters provided basic organization which surrounded the management of smart grids and monitoring usage information, it still failed to accurately detect NTL. A solution to this effect was presented in the study that used the deployment of Support Vector Machines (SVM) as an underlying classifier and combined with a real-time application interface termed Electricity Usage Classifier Interface (ELUCI) which was used in the monitoring and pre-processing instantaneous electricity usage time-series data. This model yielded a classification accuracy of 98.48% after evaluation with a root mean squared error of 0.0894 and an f-measure of 0.979. However, these results showed that after the evaluation of the model, it proved efficient in solving the problem it was designed to solve.

Kim (2021) performed an investigation into the detection of electricity theft. The study proposed a new type of DenseNet-RF model that detects power user theft. Random Forest algorithm (RF) was combined with the DenseNet algorithm to achieve this model, where DenseNet was used to automatically extract customer power usage characteristics, and the RF was used to classify

customer power abnormalities. By introducing the Synthetic Minority Oversampling Technique (SMOTE) algorithm used for imbalanced classification, the problem of imbalance of the customer power consumption data was solved, the hyper-parameters inside DenseNet were adjusted and the network model was modified to obtain a better preprocessing model. From experimental results in the work, the classification accuracy of the DenseNet-RF fusion model in the training set was about 99.97% and the classification accuracy in the test set was about 96.76%. The works reviewed in this section had issues mostly with accuracy, recall, F1-score, and missing values in the dataset. However, this led to the models discussed in the review not being accurate in the detection of energy theft. Therefore, the proposed system in this study aims to improve and correct these issues.

3. METHODOLOGY

The procedures applied for effectively detecting electricity meter bypass in Nigeria using artificial intelligence are encompassed in the respective workflow stated below. Firstly, an extensive literature review was conducted to identify the different algorithms used by researchers to solve the existing problem and the roles they played in the development of the different models. Through this review, the study aims to establish a research gap in the reviewed literature that would be solved. Furthermore, by implementing corresponding AI algorithms and training them using a dataset, an artificial intelligence model will be developed to differentiate between normal meter readings and bypassed readings. Lastly, recommendations will be made for further detection and prevention of bypasses.

3.1 Data Collection

The data was collected from the Enugu Electricity Distribution Company (EEDC). This data contains information on the electricity consumption patterns of 12000 smart meters from May 2019 to October 2021. The data collected contains customer attributes such as; time, load, unit, amount, and meter number. These attributes are described in Table 1 below;

Table 1: Customer Attributes of Dataset

S/N	Attributes	Data Description	Data Format
1	Time and date	The time for every recharge	Time and date
2	Load	Amount of electricity consumed at every recharge time.	Integers
3	Unit	The amount of electricity given at every purchase.	Integers
4	Amount	Amount paid for the purchase of the recharged units.	Integers
5	Meter number	The serial number assigned to each customer's meter.	Integers

3.2 Data Processing

This section described the approaches taken to process the data collected. Due to the large volume of data collected, it became imperative to process the data effectively. One of these approaches was data imputation which was introduced by (Rosenthal, 2017). During this phase, some missing values were identified in the data. To address this issue, the regression imputation technique which was proposed by Song and Shepperd (2007) was implemented. Implementing

this regression imputation technique helped the study estimate the missing values in the data and improve the overall quality of the data, aiding more robust analyses and insights.

3.3 Data Augmentation and Feature Extraction

Due to the limited sample size of data collected from the domain expert, data augmentation approach was utilized to increase the data volume to ensure the robustness and efficiency of the proposed ML model. The Interpolation method described in (Papadaki, 2017) is one of the techniques used for data augmentation (Badimala, et. al., 2019) and it was implemented in this study to this effect. The approach used for feature extraction in this study was Independent Component Analysis (ICA). ICA is applied to transform the original features of the data into a new set of features thereby representing them in visual form (Kwak, et. al., 2001).

3.4 Machine Learning Algorithms Used in the Development of the Electricity Meter Bypass detection system.

This section discussed the ML algorithms used in training the data collected which are; Artificial Neural Network (ANN) and Support Vector Machines (SVM).

3.4.1 Artificial Neural Networks (ANN)

Artificial Neural Network is a supervised learning algorithm that interacts with the given data to help it produce future outputs without errors (Danish & Sharma, 2015). In ANN, learning involves the adjustment of the weights of the connections among the nodes (neurons) within a specific network (López, et, al., 2022). According to Dastres and Soori, 2021, ANN is part of a computer system that mimics the activities of the human brain i.e., how it processes information. This algorithm as found in algorithm 1 is made up of some fundamental building blocks or rather features that are interconnected which are; neurons (nodes), layers, weight matrix, activation function, bias, optimization algorithms, loss/cost function, parameters, and hyper-parameters. Combining these features, ANN can learn data, make predictions, natural language processing, and decision-making. (Ravish, 2023).

3.4.2 Support Vector Machines (SVM)

SVM is used for classification and regression problems (Wang, et, al., 2017). This ML algorithm as contained in Algorithm 2 finds the best hyperplane that separates two classes (Saini, 2023). By training the SVM model with the collected and already labeled data that contains features such as; meter readings, usage patterns, and other relevant information, the algorithm was able to learn the complex relationships associated with bypassed readings enabling the model to classify the readings as “normal” and “bypassed”.

ANN: Algorithm 1

- 1: System Initialization
- 2: Weight and Bias function identification
- 3: Summation function
- 4: Hyperbolic tangent activation function
- 5: If
 - neuron is activated = true*
 - then*
- 6: Output
- 7: Else return to step 4

SVM: Algorithm 2

- 1: Load and preprocess the dataset
- 2: System initialization
- 3: Define decision function value
- 4: Train model
- 5: If
 - decision value > threshold:*
- 6: Classify as “bypassed”
- 7: Else classify as “normal”
- End

End

3.5. Development of Electricity Meter Bypass Detection Model using Algorithms 1 and 2

The data collected was imported into the Neural Network algorithm as represented in Algorithm 1 and trained using the Back Propagation (BP) which is one of the optimization algorithms for neural networks (Hamza, et. al., 2015). During the training, the data was divided into; training, validation, and test data with a ratio of 80:10:10. The back-propagation algorithm was used to adjust the weight and bias of the neurons while the error was being monitored. When the error was close to tolerance, the training stopped and the model for electricity meter bypass detection was generated. Likewise, the data collected was also imported into the Support Vector Machine (SVM) algorithm which was also a machine learning algorithm adopted in this study for the classification of the data as presented in Algorithm 2. During the training, the support vector machine algorithm drew a line to classify the dataset which is referred to as hyper-plane, and kept adjusting the weight while monitoring the error. When the error was close to tolerance, the training stopped. A model was generated for the classification of meter data to determine if it is bypassed or normal at the end of the training. Fig. 3.1 below shows the flowchart for the development of the model using Neural Networks and Fig. 3.2 shows the flowchart for the development of the model using Support Vector Machines (SVM).

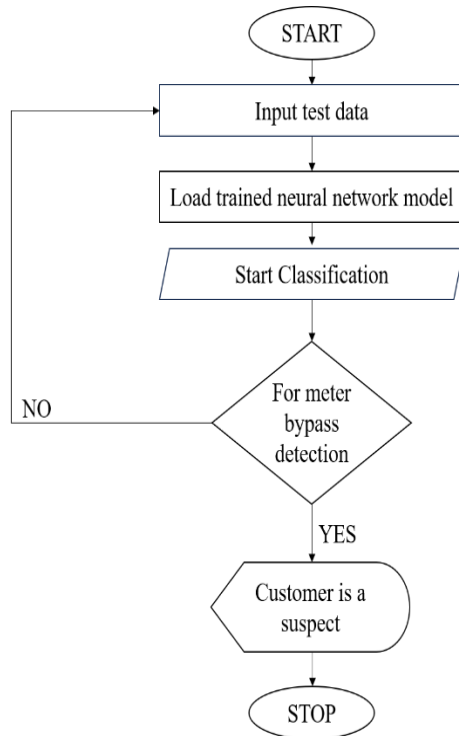


Fig. 1 Flowchart of NN-based model

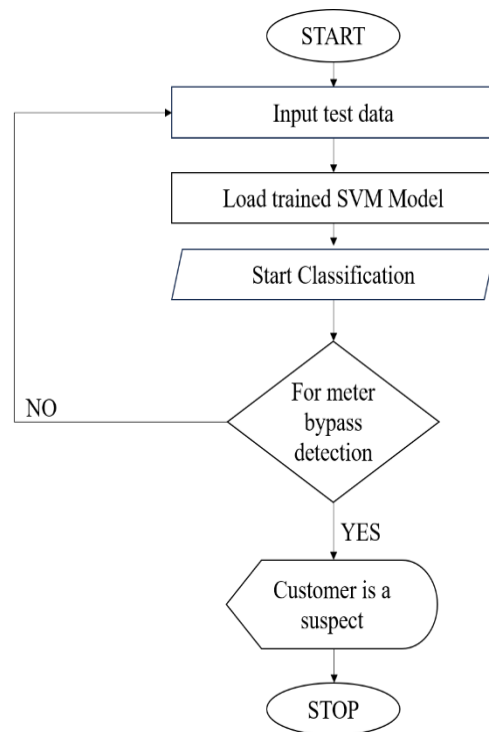


Fig. 2 Flowchart of SVM-based model

4. RESULTS AND DISCUSSIONS

This section presented the results of the training of the neural network model and the Support Vector machine-based model for the detection of electricity meter bypass. The training process for the NN-based model and SVM-based model was evaluated considering the Receiver Operating Characteristic (ROC) Curve which was used to represent the performance of the

model as the discrimination threshold varied. The ROC curve plotted the True Positive Rate (TPR) against the False Positive Rate (FPR) for different threshold values. This was used to balance the model’s decision in classifying real cases of meter bypass and flagging off false alarms. These results are presented in figure 3 and 4 for the Ann based ROC and the SVM based ROC respectively.

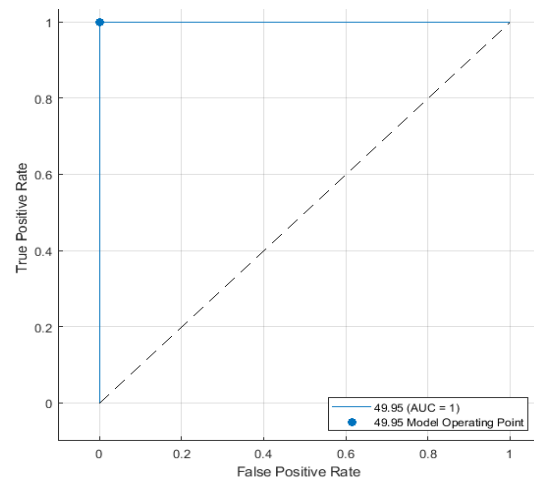
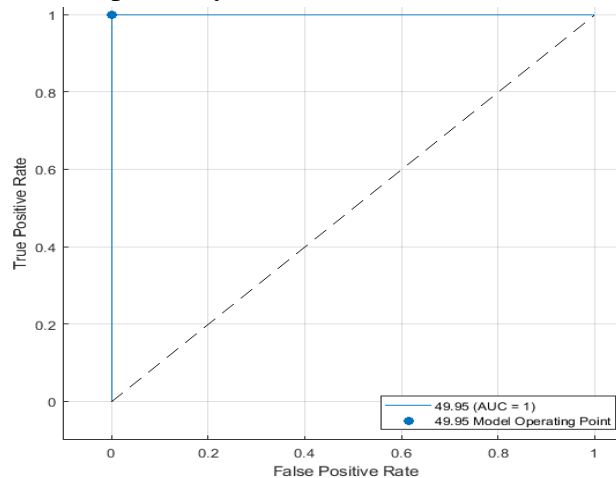


Figure 3: The ROC for NN-based model

Figure 4: The ROC for SVM-based model

From the ROC Curve result in Figure 3 & 4, the Area Under Curve (AUC) is 1. This indicates that, the models can perfectly distinguish between the negative and positive classes (in this case, between bypassed readings and non-bypassed readings). The next result used the confusion matrix to evaluate the electricity meter bypass detection model. The confusion matrix is a table that provides a clear breakdown of the model’s predictions and how well the model can classify the given data and unseen data in subsequent cases. The confusion matrix for the SVM and ANN model was presented in figure 5 and 6 respectively;

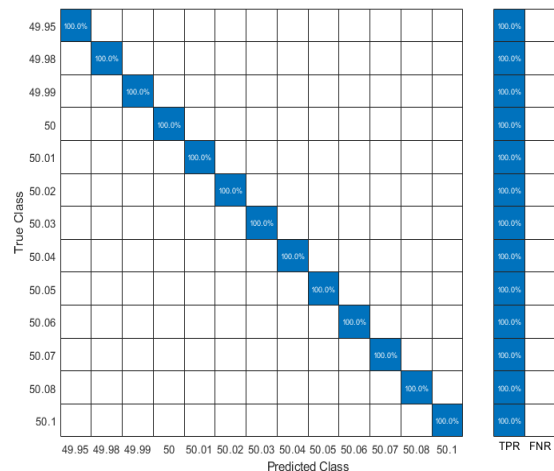
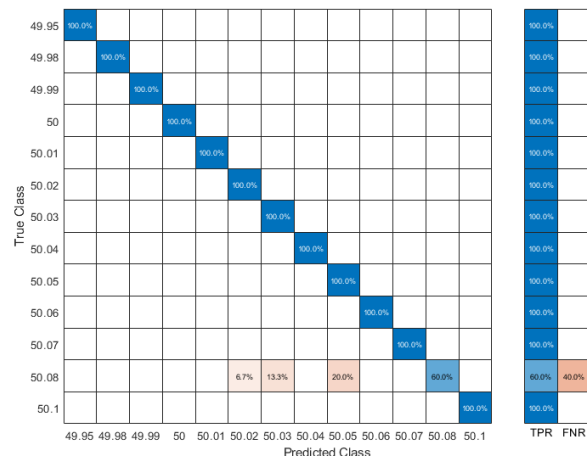


Figure 5: Confusion matrix for SVM

Figure 6: Confusion matrix NN-based model

The confusion matrix in Figure 5 provides the relationship between the true class and the predicted class. Out of the 13 classes, 12 were correctly predicted showing a True Positive Rate of 100% which indicated that the model successfully identified bypassed readings. However one of the classes showed a True Positive Rate (TPR) of 60% and a False Negative Rate (FNR) of

40%. These values indicates that the model in that case had correctly classified 60% of meter bypass cases and then 40% of incorrect classification of non-meter bypass cases respectively.

The confusion matrix in Figure 6 showed a TPR of 100% across all 13 classes which indicates that the model perfectly identified 100% of meter bypass cases. However, this means that the model could perfectly classify the electricity meter readings. In the table 2, a comparative analysis of the two model was presented;

Table 2: Comparative Analysis of the NN-based Model and SVM-based Model

ML Algorithm	Accuracy(%)	TPR(%)	FNR(%)
SVM	93.9	100	40
ANN	100	100	0

The table 2 presented comparative analysis was performed on the ML algorithms considered in this study; Artificial Neural Network (ANN) and Support Vector Machine (SVM) considering the parameters; Accuracy, True Positive Rate (TPR), False Negative Rate (FNR). After the analysis, it was observed that for Accuracy, the ANN yielded a higher accuracy of 100% while the SVM yielded an accuracy of 93.9%; both the ANN-based model and SVM-based model yielded a TPR of 100%; the SVM-based model yielded an FNR of 40% while the ANN-based model yielded 0%. Similarly, other state of the art algorithm existing were compared with the new model as reported in table 3;

Author	Technique	Accuracy (%)	TPR (%)
Bohani, et. al, (2021)	DT	91.39	2.87
	ANN	92.54	35.49
	DANN	92.31	40.94
	AdaBoost	91.75	7.57
Ullah, et. al., (2021)	CNN-GRU	83	93
	CNN-LSTM	81	93
	CNN-GRU-PSO	89	95
Petrlik, et. al., (2022)	SVM	81	
	RF	80	
	KNN	79	
	NB	68	
	LR	69	
Hussain, et. al., (2022)	KTBoost	93.38	93
Saha, et. al., (2020)	LR	76	
Aniedu, et. al., (2022)	ELUCI	98.48	
Kim (2021)	DenseNet-RF	96.76	
New System	New SVM	93.9	100
	New ANN	100	100

The table 3 is the comparative analysis of reviewed models and the new system with respect to accuracy. From the Figure, the new SVM-based model showed higher accuracy of 93.9% which is 12.9% more than the reviewed SVM-based model and the new ANN showed higher accuracy

of 100% than all the reviewed models, proving it more efficient. Furthermore, the new ANN-based model and SVM-based model showed a higher TPR of 100% than all the other reviewed models, thus implying success ability to classify customers involved in energy theft..

5. Contribution to knowledge

This study advances the understanding of how machine learning algorithms can efficiently identify instances of meter bypass and unauthorized consumption of electricity. By implementing the proposed system, utility companies can curb the revenue losses that are associated with energy theft or illegal consumption of electricity.

6. Conclusion

This study presented an electricity meter bypass detection model using SVM and ANN for the classification of the data collected from the Enugu Electricity Distribution Company (EEDC). The data was processed using the data imputation algorithm and the regression imputation technique was used to estimate missing values in the data. Furthermore, the data was augmented using the Interpolation algorithm, and the features were extracted using ICA. The performance of the models was evaluated using the AUC score and accuracy score. The SVM-based model yielded an accuracy of 93.9% and an AUC score of 1 while the ANN-based model yielded an accuracy of 100% and an AUC score of 1. When compared to other models, there was a reasonable amount of improvement. The limitation of the study is that the outcome of this prediction model still needs to be subjected to other investigation to prove that the customer is involved with energy theft.

7. Recommendations

- i. Implementation of appropriate security measures to protect the model's integrity and prevent it from being exploited or tampered with.
- ii. Feedback from utility companies and other relevant stakeholders should be gathered to make sure that the model meets their needs.

References

- Abdullateef, A.I., Slami, M.J.E., Musse, M.A., Aibinu, A.M and Onusanya, M.A. (2012). "Electricity theft prediction on low voltage distribution system using the autoregressive technique". *International Journal of Research in Engineering and Technology* vol 1 no. 5 pp 2277-4378.
- Aladeitan, O. A., and Joan, K. S. D. (2020). *Electricity Metering System in Nigeria: An Examination of the Regulatory and Policy Initiatives to Bridge the Gap*. Benue State University Law Journal. <https://bsum.edu.ng/journals/files/law/vol9/article7.pdf>
- Aniedu, A. N., Nwokoye, S. C., Okafor, C. S., and Anyanwu, K. U. (2022). "Modelling Machine Learning-based Energy Loss Detection and Monitoring System for Advanced Metering Infrastructure," 2022 5th Information Technology for Education and Development (ITED), Abuja, Nigeria, 2022, pp. 1-7, doi: 10.1109/ITED56637.2022.10051398.
- Badimala, P., Mishra, C., Venkataramana, M. K., Bukhari, S. S. (2019). "A Study of Various Text Augmentation Techniques for Relation Classification in Free Text". Researchgate. <https://www.researchgate.net/publication/331784439>. DOI:10.5220/0007311003600367
- Bohani, A. F., Suliman, A., Saripuddin, M., Sameon, S. S., Salleh, M. S. N., and Nazeri, S. (2021). A Research Article on "A Comprehensive Analysis of Supervised Learning

- Techniques for Electricity Theft Detection". Hindawi. Journal of Electrical and Computer Engineering. Volume 2021, Article ID 9136206, 10 pages. <https://doi.org/10.1155/2021/9136206>
- Bush, S. F. (2014). "Smart Grid: Communication-Enabled Intelligence for The Electric Power Grid", IEEE Press, Wiley 2014.
- Czechowski, R., and Kosek, M. A. (2016). The Most Frequent Energy Theft Techniques and Hazards in Present Power Energy Consumption. <https://www.researchgate.net/publication/309499028>.
- Dahunsi, F. M., Olakunle, O. R., & Melodi, A. O., (2021). "Evolution of Electricity Metering Technologies in Nigeria". NIGERIAN JOURNAL OF TECHNOLOGICAL DEVELOPMENT, VOL. 18, NO.2, JUNE 2021. pp 152-162.
- Danish, N., Sharma, V., and Mundari, A. D. N., (2015). " Neural Network " a Supervised Machine Learning Algorithm. IJEDR | Volume 3, Issue 2 | ISSN: 2321-9939.
- Dastres, R., and Soori, M. (2021). "Artificial Neural Network Systems". International Journal of Imaging and Robotics, [Formerly known as the "International Journal of Imaging" (ISSN 0974-0627)] Volume 21; Issue No. 2; Year 2021; Int. J. Imag. Robot. ISSN 2231-525X; Copyright © 2021 [International Journal of Imaging and Robotics.
- Hamza, M. F. Yap, H. J. and Choudhury, I. A. (2015) "Recent advances on the use of meta-heuristic optimization algorithms to optimize the type-2 fuzzy logic systems in intelligent control," Neural Computing and Applications, vol. 28, no. 5, pp. 1-21.
- Hussain, S., Mustafa, W. M., Al-Shqeerat, A. H. K., Al-rimy, S. A. B., and Saeed, F. (2022). "Electric theft detection in advanced metering infrastructure using Jaya optimized combined Kernel-Tree boosting classifier: A novel sequentially executed supervised machine learning approach" Wiley. The Institution of Engineering and Technology (IET), IET Generation, Transmission & Distribution. DOI: 10.1049/gtd2.12386
- Kim, T. (2021). "Electricity Theft Detection Using Fusion DenseNet-RF Model". International Journal of Smartcare Home Vol.1, No.1 (2021), pp.9-22.
- Kwak, N., Choi, C., Choi, J. Y. (2001). "Feature extraction using ICA". Researchgate. <https://www.researchgate.net/publication/221078415>. DOI:10.1007/3-540-44668-0_80
- Lopez, M. A. O., Lopéz, M. A., and Crossa, J. (2022). "Multivariate Statistical Machine Learning Methods for Genomic Prediction". Springer. ISBN : 978-3-030-89009-4
- Nkemneme, K. O. (2020). An article on the Impact of Electricity Theft on the Nigerian Electricity Industry. Published Nov. 12, 2020. <https://www.linkedin.com/pulse/impact-electricity-theft-nigerian-industry-nkemneme-msc-anipr-shrm>.
- Olaoluwa, G. O. (2017). "Electricity Theft and Power Quality in Nigeria". International Journal of Engineering Research & Technology (IJERT) <http://www.ijert.org> ISSN: 2278-0181. IJERTV6IS060492. Published by: www.ijert.org. Vol. 6 Issue 06, June – 2017.
- Papadaki, M. (2017). "A Thesis: Data Augmentation Techniques for Legal Text Analytics". Department of Computer Science, Athens University of Economics and Business, Athens.
- Petrlik, I., Lezama, P., Rodriguez, C., Inquilla, R., Reyna-Gonzalez, E. J., and Esparza, R. (2022). "Electricity Theft Detection using Machine Learning". International Journal of Advanced Computer Science and Applications (IJACSA). Vol. 13, No. 12, 2022.
- Ravish, R. (2023). "Components of an Artificial Neural Network". <https://www.enjoyalgorithms.com>.

- Rosenthal, S. (2017). "Data Imputation". Researchgate. [https://www.researchgate.net/publication/320928605 Data Imputation](https://www.researchgate.net/publication/320928605_Data_Imputation). DOI:10.1002/9781118901731.iecrm0058.
- Saha, S., Chakraborty, U., Biswas, H., Galib, R. I., and Degadwala, S. (2020). Using Machine Learning Analytics to Detect Abnormalities and Electricity Theft. International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSCEIT). ISSN: 2456-3307 (www.ijsrcseit.com) doi: <https://doi.org/10.32628/CSEIT206552>.
- Saini, A. (2023). "Guide on Support Vector Machine (SVM) Algorithm". Analytics Vidhya. <https://www.analyticsvidhya.com/blog/2021/10/support-vector-machinessvm-a-complete-guide-for-beginners/> Published On October 12, 2021, and Last Modified On July 7th, 2023.
- Song, Q., and Shepperd, J. M. (2007). "Missing Data Imputation Techniques". Researchgate. International Journal of Business Intelligence and Data Mining 2(3):261-291 DOI:10.1504/IJBIDM.2007.015485
- The Sun (2022). A Press Release by Mr. Emeka Ezeh, Head, of Corporate Communications, EEDC on the increasing rate at which some of its customers engage in acts of energy theft, especially meter bypass. Published on 17th January 2022. <https://sunnewsonline.com/eedc-decries-increasing-rate-of-energy-theft-meter-bypass-by-customers/>
- Ullah, A., Javaid, N., Yahaya, S. A., Sultana, T., Alzahrani, A. F., and Zaman, F. (2021). "A Research Article: A Hybrid Deep Neural Network for Electricity Theft Detection Using Intelligent Antenna-Based Smart Meters". Hindawi. Wireless Communications and Mobile Computing Volume 2021, Article ID 9933111, 19 pages <https://doi.org/10.1155/2021/9933111>
- Wang, H., Xiong, J., Yao, Z., Lin, M., and Ren, J. (2017). "Research Survey on Support Vector Machine". <https://eudl.eu/pdf/10.4108/eai.13-7-2017.2270596>