ABUAD Journal of Engineering Research and Development (AJERD)
ISSN (online): 2645-2685; ISSN (print): 2756-6811

Volume 7, Issue 2, 317-328

Developing and Implementing an Artificial Intelligence (AI)-Driven System For Electricity Theft Detection

Nwamaka Georgenia EZEJI[1], Kingsley Ifeanyi CHIBUEZE[2], Nnenna Harmony NWOBODO-NZERIBE[1]

[1]*Department of Computer Engineering, Enugu State university of Science and Technology, Enugu State, Nigeria*
georgeniaezeji@yahoo.com/nnenna.nwobodo@esut.edu.ng

[2]*Department of Computer Science & Mathematics, Godfrey Okoye University, Enugu State, Nigeria*
chibueze_kingsley@gouni.edu.ng

Corresponding Author: georgeniaezeji@yahoo.com, +2348032657047
Date Submitted: 23/07/2024
Date Accepted: 04/09/2024
Date Published: 15/09/2024

***Abstract**: Electricity theft is a significant challenge for utility companies worldwide, leading to substantial economic losses and inefficiencies in power distribution. Traditional methods of detecting electricity theft, such as manual inspections and routine audits, are often inefficient and ineffective. To address this issue, this study aims to develop and implement an artificial intelligence (AI)-driven system for electricity theft detection. Methodology used are data collection, data analysis, feature selection with Chi-Square, feature transformation with Principal Component Analysis (PCA), Support Vector Machine (SVM) and model for electricity theft detection. To achieve this, a Particle Swarm Optimization Algorithm (PSO) was applied to improve training performance of the SVM, using data of meter recharge information collected from Enugu Electricity Distribution Company (EEDC). The system effectiveness is validated through extensive testing using real-world data from various regions and scenarios, demonstrating its robustness and adaptability. The system result considering FDR reported that 0.11 was achieved for the particle swarm based SVM model. When TPR was considered for analysis, it was observed that particle swarm based SVM attained a score of 0.89. In addition, Particle swarm based SVM attained PPV of 0.895. In terms of accuracy, the particle swarm based SVM reported an accuracy of 0.857. The result showed that the particle swarm based SVM performed better from the system validation achieved through comparative analysis, hence it is recommended for use to develop the new software for energy theft investigation. The implementation of this AI-driven solution offers numerous benefits, including enhanced detection accuracy, reduced operational costs, and improved overall efficiency of power distribution networks. Moreover, it enables utility companies to take proactive measures to prevent theft, ensuring a more reliable and secure electricity supply for consumers.*

***Keywords:** Electricity Theft, Artificial Intelligence, Support Vector Machine, Principal Component Analysis, Particle Swarm Optimization Algorithm*

1. INTRODUCTION

Electricity theft characterized by the unauthorized use of electrical power, poses a significant challenge to utility companies worldwide. This illegal activity results in substantial economic losses, estimated at billions of dollars annually, and undermines the efficiency and reliability of power distribution networks. While the government often subsidizes power supply, it is not provided for free. Regrettable, [1] submitted that certain private individuals, enterprises, and organizations resort to illegal means to access electricity without payment by bypassing the proper channels (power theft).

According to Gbolahan [2], power theft refers to the unlawful consumption of electrical energy without proper payment or permission. Traditional methods of detecting electricity theft, such as manual inspections, routine audits, and basic data analysis, are often inadequate due to their labor intensive nature and limited accuracy. As electricity consumption patterns become increasingly complex, there is a pressing need for more sophisticated and automated approaches to identify and mitigate theft. The advent of smart meters and advanced metering infrastructure (AMI) has revolutionized the way electricity usage is monitored and recorded [3, 4]. These technologies generate vast amounts of granular data, providing an opportunity to employ advanced analytical techniques for theft detection. However, the sheer volume and complexity of the data present significant challenges for traditional analytical methods. This is where Artificial intelligence (AI) comes into play, offering powerful tools to analyze large datasets, identify patterns, and detect anomalies indicative of theft.

This paper on developing and implementing an Artificial Intelligence (AI)-driven system for electricity theft detection is aimed to develop a system that can automatically identify and detect instances of electricity theft in real time. This would help to reduce financial losses for electricity companies and improve the reliability of the electricity grid

.

2. LITERATURE REVIEW

This section presents review of relevant literatures considering various artificial intelligence techniques adopted for detection of electricity theft through meter bypass. The scholars [2] developed a detection system for electricity theft using a machine learning technique. The work utilized data from smart electrical meters belonging to the State Grid Corporation of China, which supplies approximately 1.1 billion users across the national territory. The investigation focused one valuating the performance of five machine learning models which are Support Vector Machine (SVM), K-Nearest Neighbor (K-NN), RandomForest (RF), Logistic Regression (LR), and Naïve Bayes (NB) and applied for the detection of electricity theft. The accuracy rates of the models were reported as follows: 81% for SVM, 79% for K-NN, 80% for RF, 69% for LR, and 68% for NB. Consequently, the study recommended the application of SVM in future research, even though the accuracy leaves room for improvement. The scholars [5] developed a Recursive Feature Elimination (RFE) based feature selection and K-Nearest Neighbour Oversampling (KNNOR) based data balancing system for electricity theft detection. The system employed a Bidirectional Long-Short-term Memory (BiLSTM) and LogitBoost stacking ensemble model. The system's functionality consisted of four stages: data pre-processing, feature extraction, data balancing, and electricity theft classification. The training and testing data sets were obtained from the state grid corporation of China's electricity consumption data. The performance of the proposed technique achieved an accuracy of 89.45% in electricity theft detection, however despite the success, there is room for improvement.

Electricity theft detection system using the XGBoost algorithm was presented by Mhaske et al. [6]. The system utilizes XGBoost and Optical Character Recognition (OCR) techniques to analyze data based on customers' consumption patterns recorded in the Advanced Metering Infrastructure (AMI). The goal is to detect non-technical losses in the electrical system and identify them as theft. The results of the system indicate that XGBoost, along with the OCR technique, provides accurate results with reduced time consumption. However, a practical validation of the model would have improved the reliability. Onibonoje [7] presented an IoT-based approach for the protection and billing of residential energy meters. The study focused on the real-time monitoring and management of residential, vendor, and consumer power systems through the meter using IoT technology. A user-friendly web-based platform was developed for various applications such as online meter recharge and remote control of user access to power for defaulting customers. However, the study did not mention electricity theft, which is the crust of the principal study. Reshma et al. [8] conducted research on the implementation of machine learning for electricity theft detection. Their system utilized a green scheme to discover power robbery, computer payments, and display power loads without compromising customer privacy. This was achieved by analyzing data from smart meters running on an advanced metering infrastructure. In addition, symmetric encryption utilizing the k-means algorithm was applied to encrypt meter readings and customer information. Furthermore, Convolutional Neural Network (CNN) model was utilized to learn features from the data on an hourly and daily basis and generated a model which was used for the calculation of energy consumption. The model was deployed into Atmega 328 using Octocoupler device for the calculation of electricity units consumed. The result of the information generated from the system was stored to the cloud using NodeMcu. While this study made great contribution to energy management, it did not directly address the problem of energy theft.

The researchers [9] conducted a comprehensive analysis of supervised learning techniques for the detection of electricity theft. The study aimed to evaluate the performance of various supervised learning techniques for detecting electricity theft. The dataset used for the study was acquired from the State Grid Corporation of China (SGCC). The techniques considered in the study were artificial neural network [10], decision tree, deep artificial neural network, and AdaBoost. The analysis revealed accuracies of 91.77% (decision tree), 92.74% (artificial neural network), 93.04% (deep artificial neural network), and 91.67% (Ada Boost). Deep artificial neural network was recommended as the best model; however, practical validation of the model can be used to enhance the trustworthiness. Chen et al. [18] presented an electricity theft detection model using a residual neural network for smart meters. The model considered the weekly electricity records and statistical features of the weekly power consumption data extracted using the ResNet model. Deep residual network classifier models were employed for theft detection. The presented electricity theft detection model achieved a detection rate of 97.92% with a training time of 606.79 seconds. However, practical validation of the model can be used to enhance the trustworthiness. Liu et al. [19] presented a fault-tolerant and privacy-preserving electricity theft detection system. The system utilized n-source anonymity and a convolutional neural network (CNN) to ensure the privacy of electricity data during the theft detection process. The research showed that the model achieved an accuracy of 92.86% in detecting electricity theft using the dimensionality reduction method. However, the accuracy can be improved in further studies. Madhure et al. [20] conducted research on the application of Convolutional Neural Network-Long Short-Term Memory (CNN-LSTM) for electricity theft detection in advanced metering infrastructure. The study utilized a dataset from the Irish Social Science Data Archive (ISSDA) published by the Commission for Energy Regulation of Ireland. The dataset consisted of energy consumption data from 5000 users collected over a 2-year period, including residential consumers and small to medium-sized industries. Rectified Linear Unit was applied as the activation function in the deep learning algorithms. The test results demonstrated a detection accuracy of 97% and a mean square error rate of 0.01426 which is good, however, practical validation of the model can be used to enhance the trustworthiness.

Ullah et al. [21] introduced a hybrid deep neural network model for electricity theft detection using intelligent antenna-based smart meters. The system employed a dataset acquired from the State Grid Corporation of China and implemented smart antenna-based meters on the consumer side. The feature extraction process utilized a convolutional neural network, and the classification operations were performed using a particle swarm optimization-gated recurrent unit model (PSO-GRU). The hybrid deep neural network model presented in the study achieved an accuracy of 87% which is good, but the accuracy leaves room for optimization in further studies. Ayub et al. [22] proposed the application of a Convolutional Neural Network-Gated Recurrent Unit (CNN-GRU) and Manta Ray Foraging Optimization (MRO) algorithm for electricity theft detection. The study utilized the swarm-based optimization algorithm MRO to tune the hyperparameters for CNN-GRU feature extraction and classification. To effectively identify power stealing users under-represented in the datasets, the Synthetic Minority Oversampling Technique (SMOTE) was employed. The dataset used in the study was acquired from China National Grid Co. Ltd and comprised 10,000 customers. The system achieved an accuracy of 91.1% in electricity theft detection. However, practical validation of the model can be used to enhance the trustworthiness.

Syed et al. [23] presented a study on using electricity consumption patterns for the detection of energy theft in a smart energy grid. The system focused on detecting meter tampering at the smart meter level of the power distribution system, utilizing deep learning, specifically Long Short-Term Memory (LSTM) algorithm, to develop a data-driven approach for efficient energy theft detection. The data used for this study was acquired from the Smart Grid Corporation of China (SGCC), comprising 42,372 customer data points. The study reported an accuracy of 92.69% for the LSTM algorithm in detecting energy theft. However, the model was not validated practically, which is vital and remain a gap. Nabil et al. [24] presented a deep recurrent electricity theft detection method in advanced metering infrastructure networks using random tuning of hyper-parameters. The study employed a Gated Recurrent Unit-Recurrent Neural Network (GRU-RNN) to exploit the time-series nature of electricity consumption rates and improve the detection performance. The detection technique utilized random search analysis to determine suitable stages for fine- tuning the hyper-parameters. The system was trained and tested with 107,200 real energy consumption days of data from 200 consumers. The results showed that the technique achieved a detection rate of 93% and a false acceptance rate of 5%, which is good, however, practical validation of the model can be used to enhance the trustworthiness.

3. MATERIALS AND METHODS

3.1 Materials

The materials required to model and implement an AI Based electricity theft detection system include data, hardware and software requirements.

3.1.1 Hardware requirements

i. LAPTOP to train and deploy the AI model (Hp Elite Book 840 G5 Intel Core I5-16GB RAM/256GB SSD/Backlit Keyboard/FP Reader Windows 11 Pro),
ii. 1.5KVA Inverter system for power supply;
iii. 5G router which provided internet access for data collection.
iv. IN-100RFsensor
v. Tuya smart power sensor

3.1.2 Software requirements

i. Python
ii. Javascript
iii. Data of customer meter research information
iv. Google colab

3.2 Methods

The methods employed for modelling and implementing an AI electricity theft detection system include data collection, data analysis and preparation, feature selection, feature transformation and the machine learning model training and model evaluation. The machine learning algorithm considered for the detective system is the Support Vector Machine (SVM) algorithm which will be trained using Particle Swarm Optimization Algorithm.

3.2.1 Data collection

Data of customer meter information was collected from the EEDC, headquarter office, at Okpara, avenue, Enugu State, Nigeria. The data was collected considering subscriptions made by customers in Obiagu district, Enugu in the year 2021 and 2022. The instruments used for the data collection are the IN-100 RF communications sensor and Tuya-smart power sensor used to monitor the energy consumption level of the user. The population size of data collection is 12,466 customers, with 16 attributes of meter information such as serial number, date, transaction ID, login, account, and serial number, type of transaction, tariff, substation, token, power (w/h), electricity, vat, wallet, amount, and district. The total sample size of data collected is 2,119,322-meter records information.

3.2.2 Data analysis and preparation

The data preparation method applied was the integration of the dataset collected using the joining technique of data integration [11]. According to Johnson et al. [12], the joining technique is specialized in merging datasets which has the same attributes as identifiers. This technique was applied considering the similar attributes of the customer meter recharge information and then merges as a single dataset used for the research. The flow chart in the Figure 1 presented the process for the data integration

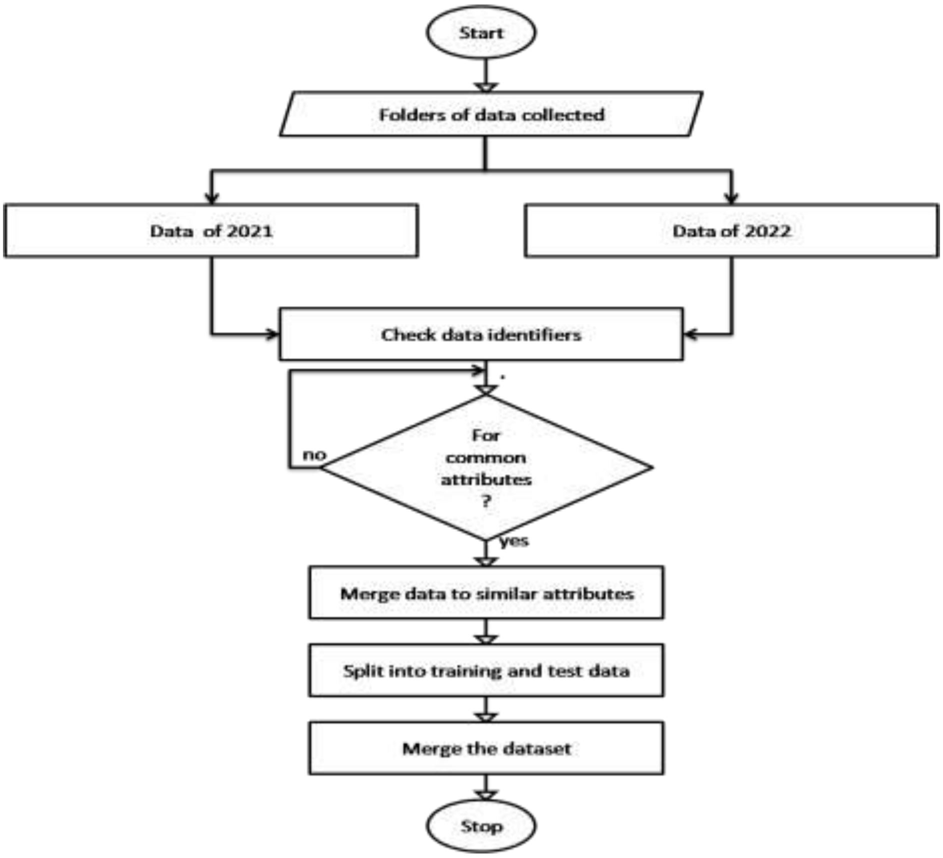

Figure 1: Flow chart of the data integration process

The Figure 1 presented the flow chart operation of the data integration process used to merge the customer data collected from 2021 and 2022 as one dataset. The process identified common attributes of the data headers and then used to merge the data. Overall, the dataset was divided into training and test set in the ratio of 80:20 and then merged as the dataset for this research.

3.2.3 Feature selection with chi-square approach

Feature selection was utilized in this study to improve the quality of the data collected, model generation, cost reduction and address over-fitting during the training process of machine learning algorithms through dimensionality reduction. The feature selection technique utilized in the study is the chi-square approach [13]. The step-wise approach of chi-square is presented as;

Algorithm 1: Stepwise of the Chi-square algorithm

1. Chi-square test: measure dependence between observed and expected frequency variable
2. Data structure: Identify categorical values of data
3. Target variable: test target variables
4. Compute p value: compute probability of null hypothesis
5. Set significance value: compare p with set threshold
6. Select features: identify variables with significant p value
7. Return features: return output as selected features

This Chi-square focuses on the statistical dependencies of the data features to identify the most important and then prioritize in the dataset. This was achieved applying equation 1 to determine the features that are most relevant based on their chi-square probability score and then select as the most important attributes for energy theft detection [14].

$$Chi - square\ (X^2) = p = \sum \left[\frac{O - E^2}{E}\right] \quad (1)$$

Where O is he observed frequency of data in each cell, E is the expected frequency and p is the output of the chi-square test.

3.2.4 Feature transformation

Feature transformation is a process used in this work to modify the data features and create new representation which is most suitable for identification by machine learning algorithms. The feature transformation algorithm adopted for the data is the Principal Component Analysis (PCA) [15]. This PCA was applied to reduce the dimension of the dataset while retaining the quality of features using the steps in the algorithm 2;

Algorithm 2: Principal Component Analysis (PCA) Algorithm [16].

```
1.  Input: Dataset X
2.  Output: Reduced-dimensional data Y
3.  Input: X, a dataset or data points.
4.  For each feature, subtract the mean and divide by the standard deviation
5.  Calculate the covariance matrix, C, of the standardized data X.
6.  Compute the eigen-values (λ) and eigenvectors (v) of the covariance matrix C
7.  Define the number of components to keep k.
8.  Select the first k eigen-values and their corresponding eigenvectors.
9.  Calculate the new data Y by multiplying X by the selected eigenvectors.
10. End
```

3.2.5 The support vector machine (SVM) algorithm

The SVM algorithm operates by searching for the perfect hyper-plane between the data points, while maximizing the class margins. It identified the supports vectors from the dataset sampled which are the closest data to the decision boundary and then build hyper-plane based using the equation 2.

$$(x) = \beta_0 + \beta_1.x_1 + \beta_2.x_2 + \cdots + \beta_n.x_n \tag{2}$$

Where (x) is the decision function which defined the class data point x, β_0 is the intercept that adjusts the hyper-plane along the y-axis, $\beta_{1,2}$,......β_n are the hyper-plane coefficients for each data samples of x_1, x_2,...x_n. The equation 2.1 was used to determine the best hyper-plane between the classes of dataset. The trained SVM with the fixed hyper-plane was used to solve future classification or regression problem. The algorithm is presented as algorithm 3.

Algorithm 3: SVM Algorithm

```
1.  Start
2.  Initialize parameters, such as learning rate ($\delta$) and regularization strength (C).
3.  Randomly initialize weights (w) and bias (b).
4.  Iterate until convergence:
5.  For each training data sample (x, y):
6.  Score = w∗x+b; Margin = y∗score %Compute score and margin
7.  If
8.  Margin<1
        a.  Apply w = w – δ ∗ (w−C ∗ y ∗ x) %Update weights:
        b.  Apply b = b + δ ∗ C ∗ y %Update bias
9.  Else:
        a.  Apply w = w- δ * w # Update weights
10. Repeat the iteration process until convergence
      a.  Optimize weights (w) and bias (b)
      b.  Determine the decision boundary of the data points
      c.  Determine the separating hyper-plane with equation
11. End
```

The optimization algorithm that was used to train machine learning algorithm. To this end, the research employs the optimization of hyper-parameters considering the particle swarm optimization algorithm.

3.2.6 Particle swarm optimization algorithm (PSO)

The PSO is another popular optimization algorithm which is very good in solving multi objective constraint optimization problem like hyper-parameter selection and optimal value assignment. The PSO determined the population of particles swarms and then used fitness computation to determine the best particle, its position and velocity. This process continued iteratively while the position and velocity of the swarm keeps updating until the best particle is determined. The model used for the fitness swarm determination is presented as [17];

$$fitness(ppo) = f(ppo) = (ppo[0] - a)^2 + (ppo[1] - b)^2 + \cdots + (ppo[n] - c)^2 \tag{3}$$

Where ppo the particle position in a 2D space is, while $a,\ b$ and c are constant parameters. While the new position of the i particle N_{Pi} is presented as Equation 4;

$$N_{Pi} = C_{Pi} + N_{Vi} \tag{4}$$

Nvi is the new velocity of the i particle, Cpi is the current position of the particle and the new velocity of i particle is presented as Equation 5;

$$N_{vi} = w * O_{vi} + c_1 * r_1 * (pbesti - C_{pi}) + c_2 * r_2 * (gbest - C_{pi}) \tag{5}$$

N_{vi} is the new velocity of the i particle, O_{vi} is the old velocity of the previous i particle, w is the weight of the particle, c_1 and c_2 are the constant acceleration while r_1 and r_2 are the random values of the particles with range [0,1], $pbesti$ is the best position of particles and C_{pi} is the current position of the particle and $gbest$ is the new best particle position. The PSO algorithm is presented as algorithm 4, while Figure 2 presented the flow chart;

Algorithm 4: The PSO algorithm

```
Start
Parameter initialization
Perform fitness of $f(ppo)$ $\#compute\ gbest$ and $pbest_i$
Determine $pbesti$ and $gbest$
For better $f(ppo)$ = $true$
Update particle position
For better $N_{vi}$=true
Update particle velocity
End for
Return $pbesti$ and $gbest$
Do
Until $pbesti$ and $gbest$
End Do; End For;
Stop
```

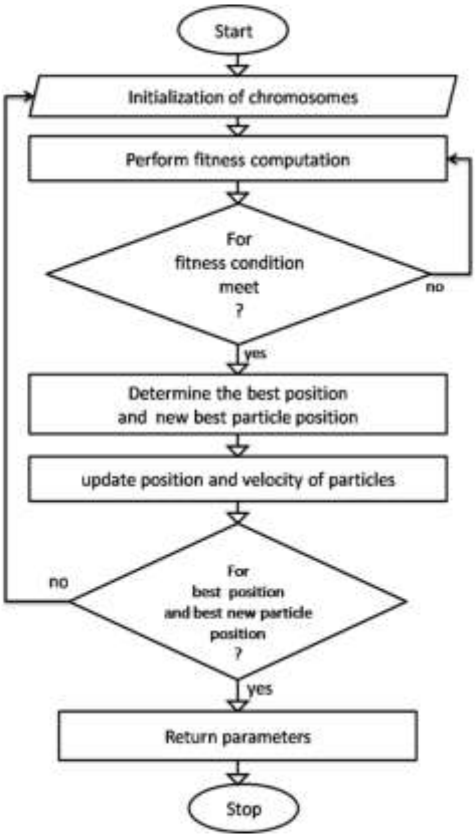
Start
Initialization of chromosomes
Perform fitness computation
For fitness condition meet ?
no
yes
Determine the best position and new best particle position
update position and velocity of particles
no
For best position and best new particle position ?
yes
Return parameters
Stop

Figure 2: Flowchart of the PSO algorithm

The PSO algorithm in the Figure 2 computes the population of swarms and then determines their fitness for the new particle position. Then the particle position and velocity is determined and updated. When a better new velocity of particle is determined and also new position, to update the parameters and the process continued until the best particle and new best position is determined and then returned as output of the process

3.2.7 Model training

This part of the work focused on training the optimized SVM algorithms developed for the generation of energy theft classification model. To achieve this, the data collected was transformed using the PCA algorithm and then feed to the SVM in algorithm 3, which then initializes the hyper-parameters and then applied the optimization based hyper parameter selection algorithm developed with PSO to train the SVM. During the training phase, the score of the weights and margin was used to determine the decision boundary hyper plane and the support vectors.

```
Algorithm 5: Particle Swarm based SVM
1.  Start
2.  Initialize parameters, such as learning rate ($\delta$),weights (w) and bias (b) and regularization
    strength (C)

3.  Apply particle swarm algorithm % for optimal hyper-parameter selection
4.  Start training iteration
5.  For each training data sample (x,y):
a.  Score =$w*x+b$; %Compute score

b.  Margin = $y*score$ %Compute margin

6.  If Margin<1
a.  Apply w= $w-\delta*(w-C*y*x)$ %Update weights:
b.  Apply b = $b+\delta*C*y$ %Update bias
7.  Else:
a.  Apply w= $w-\delta*w$# Update weights

8.  Repeat the iteration process until convergence
9.  Optimize weights (w) and bias (b)
10. Determine the separating hyper-plane
11. End
```

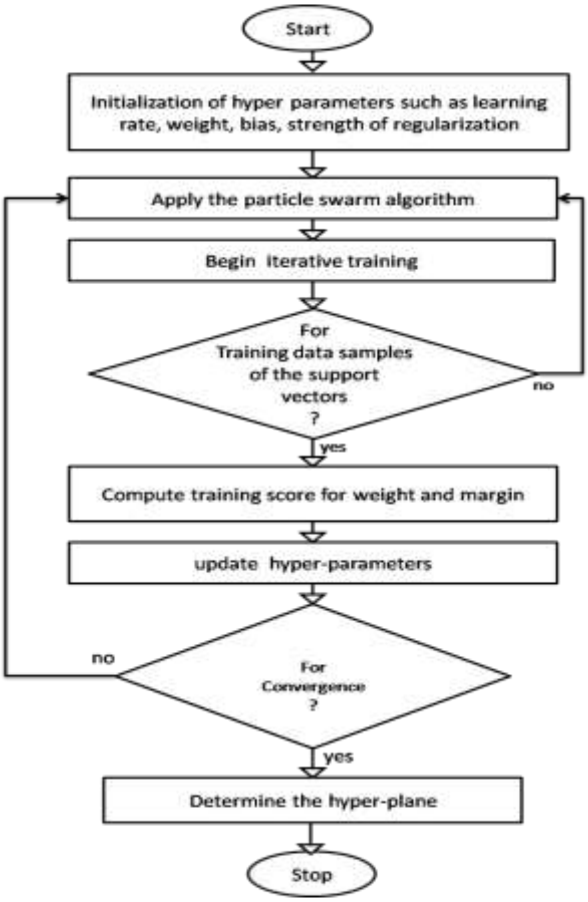
Start
Initialization of hyper parameters such as learning rate, weight, bias, strength of regularization
Apply the particle swarm algorithm
Begin iterative training
For Training data samples of the support vectors ?
no
yes
Compute training score for weight and margin
update hyper-parameters
no
For Convergence ?
yes
Determine the hyper-plane
Stop

Figure 3: Flowchart of PSO based SVM

In the algorithm 5; the PSO based SVM pseudo code was presented, showing how the SVM after the initialization of the hyper-parameters applied the PSO for the optimal selection and adjustment while training to determine the best hyper-plane which separated the support vectors and then generate the classification model. The flow chart in the figure 3 showed the process work flow of the PSO based SVM as it applies the particle swarm strategy to select the best hyper-parameters and generate the SVM model.

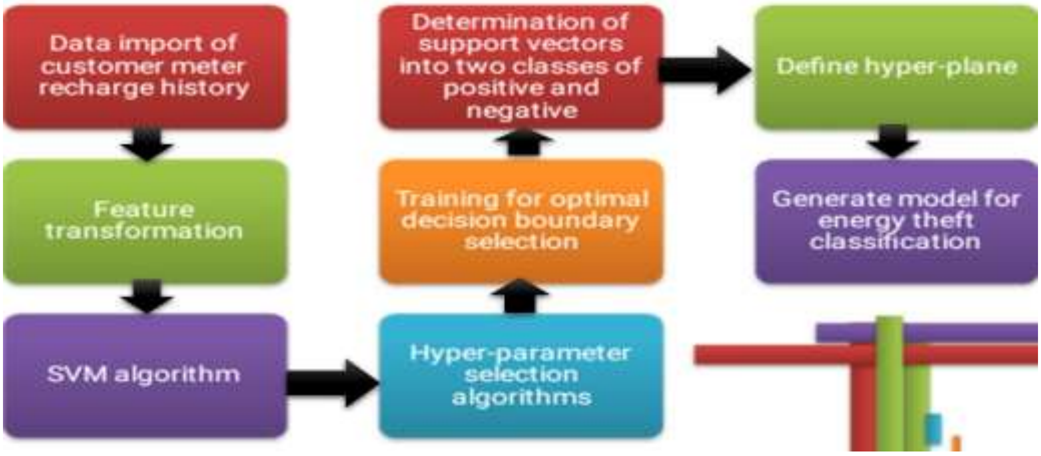
Data import of customer meter recharge history
Feature transformation
SVM algorithm
Hyper-parameter selection algorithms
Training for optimal decision boundary selection
Determination of support vectors into two classes of positive and negative
Define hyper-plane
Generate model for energy theft classification

Figure 4: Block diagram of optimized SVM training for energy theft classification

The Figure 4 presents the block diagram of the SVM training using the particle swarm optimization algorithm for the selection of hyper-parameters during the training process. While the parameters are optimally selected, the score of the weights and margins are used to determine the decision boundary which is the hyper-plane and then determination of the support vectors. While the training continued, the scores are monitored considering the positive and negative classes, until the hyper-parameters converge and then the SVM model generated for the classification of energy theft. The flow chart of the model was presented in the Figure 5;

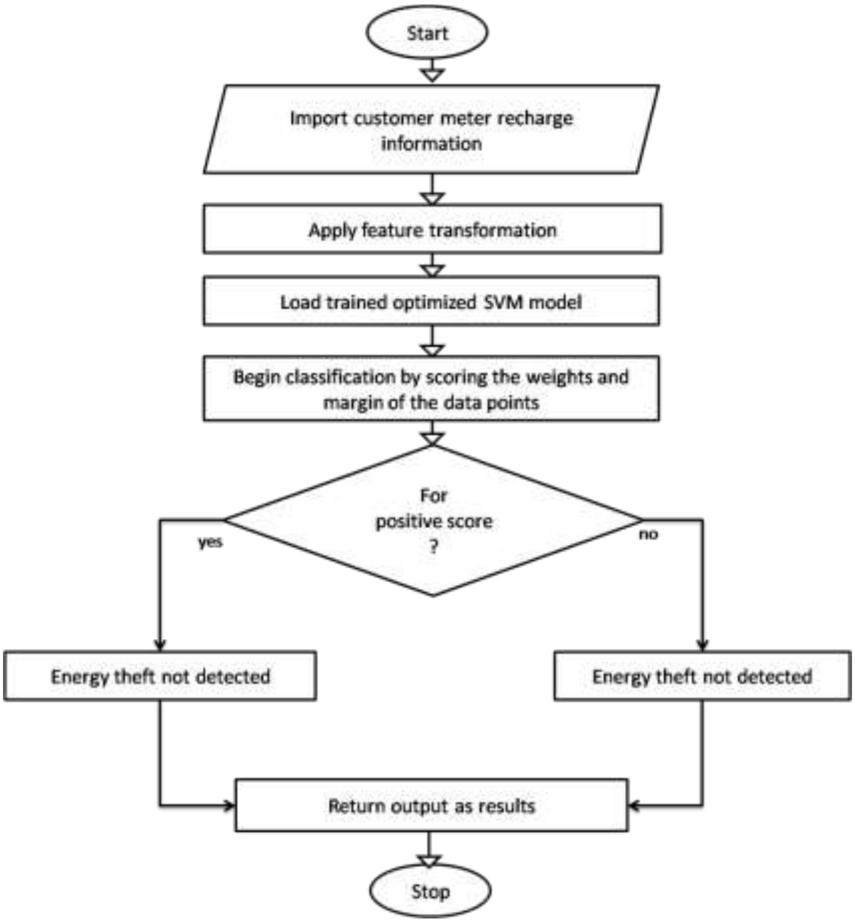
Start
Import customer meter recharge information
Apply feature transformation
Load trained optimized SVM model
Begin classification by scoring the weights and margin of the data points
For positive score ?
yes
no
Energy theft not detected
Energy theft not detected
Return output as results
Stop

Figure 5: Flowchart of SVM based model for intelligent energy theft investigation model (IETIM)

The Figure 5 presents the IETIM achieved with the trained SVM algorithm. In the beginning of the flow chart, the data of customer meter recharge information was imported and the features transformed into the trained SVM algorithm for classification of energy theft. To achieve this, the trained SVM assigned scores to the data points that are used to determine the class of the hyper-plane it belongs. When these score are positive, then it belongs to the class of none electricity theft, while when the scores are negative, electricity theft is detected and returned as output.

4. DISCUSSION OF RESULTS

The result of the SVM training displayed the training performance of the particle swarm based SVM, considering accuracy, false positive rate, false detection rate, true positive and confusion matrix respectively.

4.1 Result of the Particle Swarm Optimization based-SVM

The Particle Swarm based SVM was applied in experiment to optimize hyper-parameter selection of SVM. The process involves defining a fitness function that evaluates the SVM model's performance given specific hyper-parameters. The Particle Swarm optimization algorithm iteratively updates a population of potential solutions based on the performance evaluation until a satisfactory solution is found or a stopping criterion is met. To evaluate the training performance, PPV, FDR, accuracy, regression, FPR and TPR were employed as shown in the Figure 6.

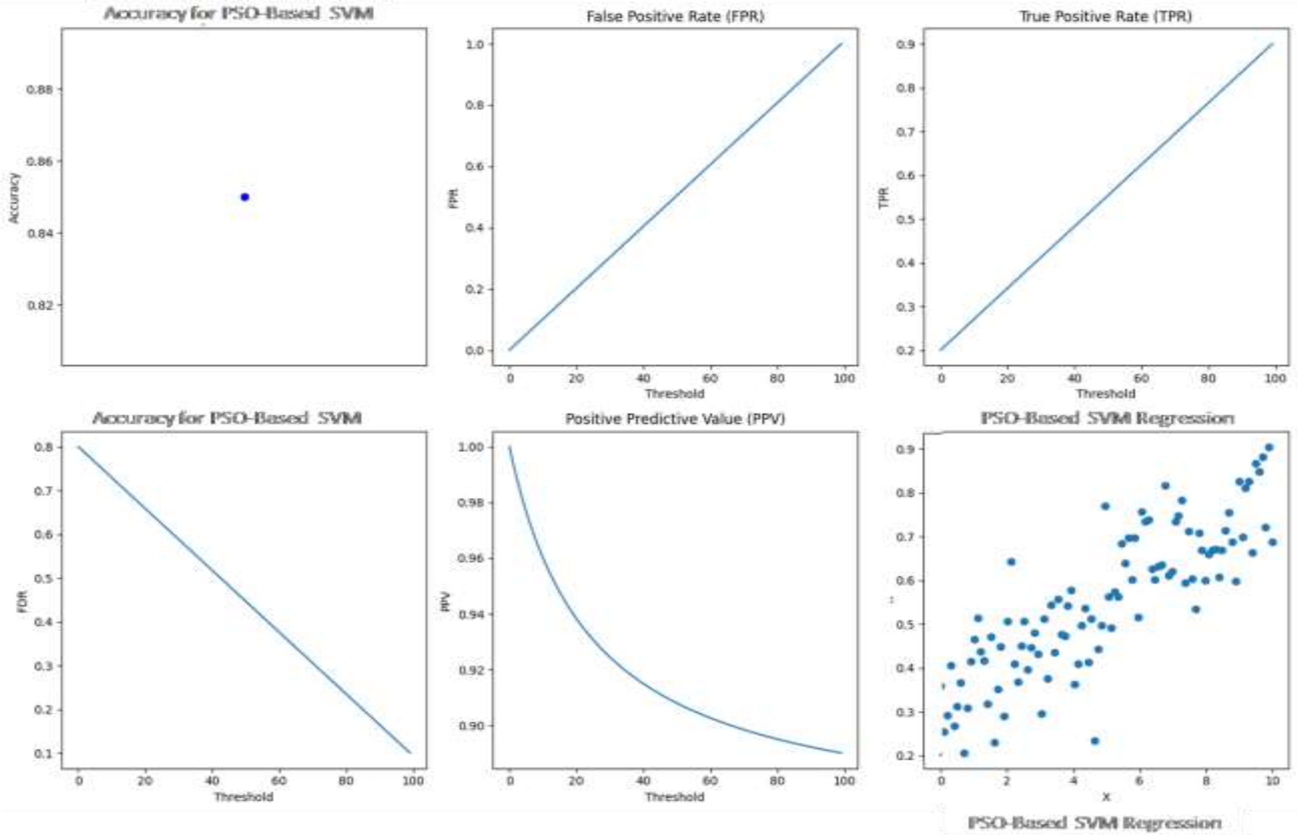

Figure 6: Results of the particle swarm based SVM training

From the Figure 6, the results for accuracy reported 0.857, TPR recorded 0.89, FPR recorded 0.98, PPV scored 0.895 respectively. This results overall, implied that the application of particle swarm optimization based SVM in the classification of customers involved in energy theft suggests that the model exhibits strong predictive capabilities, particularly in correctly identifying instances of energy theft (as indicated by the high TPR and PPV scores) while maintaining a relatively high overall accuracy. Nonetheless, these initial findings highlight the potential effectiveness of utilizing particle swarm optimization based SVM for the crucial task of detecting and mitigating electricity theft among customers.

Table 1: Result of the SVM training performance

SVM	Accuracy	FPR	TPR	FDR	PPV	Regression
PSO based	86%	0.98	0.89	0.110	0.895	0.854

4.2 Comparative Analysis with other State of the Art Algorithms

The Table 2 compared the performance of the new system with the existing model. The comparative analysis considered the new model developed with other state of the art existing models for energy theft investigation. In the analysis, accuracy was singled out as a key metrics to assess the model classification performances. These results were graphically presented in figure 7 for better analysis.

Table 1: Comparative analysis with other state of the art algorithms

Authors	Technique	Accuracy (%)
Javaid et al. [5]	Ensemble Model	89.45
Bohani et al. [9]	DT	91.77
	ANN	92.74
	D-NN	93.04
	AdaBoost	91.67
Liu et al. [19]	Privacy-Preserving Method	92.86
Ullah et al. [21]	Hybrid Deep Neural Network	87.00
Chen et al. [18]	Residual Neural Network	97.90
Madhure et al. [20]	CNN-LSTM	97.00
Ayub et al. [22]	CNN-GRU	91.10
Syed et al. [23]	Deep Learning	92.69
Nabil et al. [24]	Deep Recurrent Network	93.00
New study	PSO based SVM	86.00

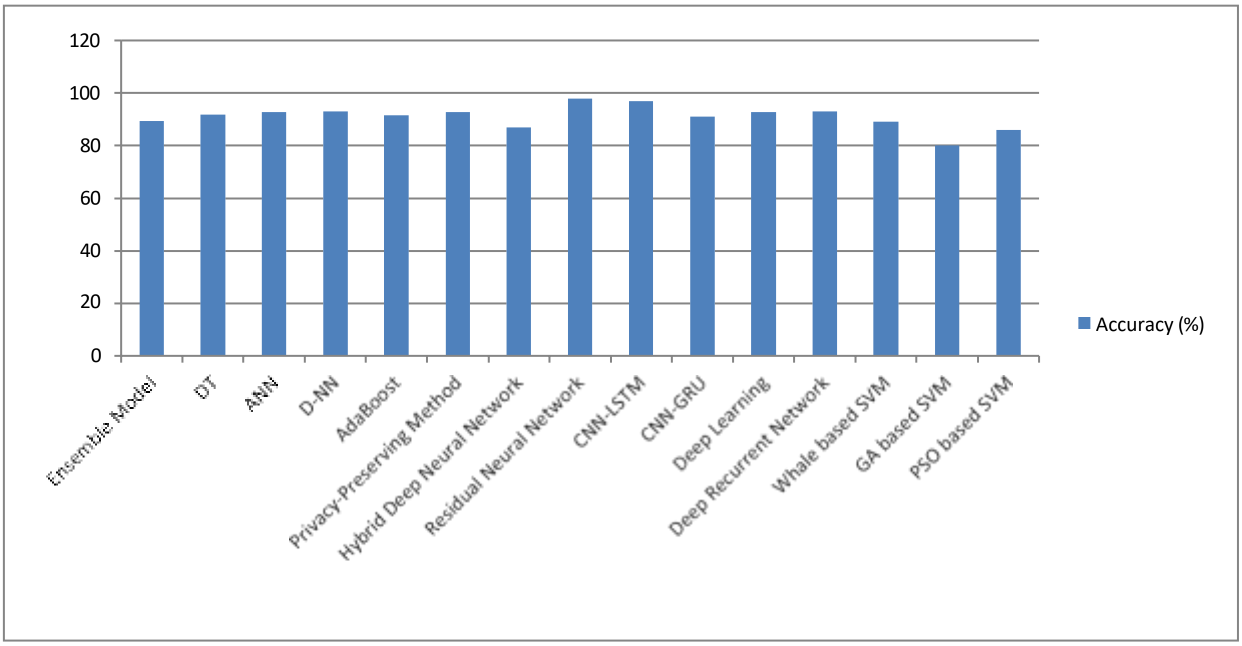

Figure 7: Comparative accuracy results

The Figure 7 showcased the comparative analysis of the existing systems with the new model considering accuracy. From the analysis, it was observed that the new model competes with the existing deep learning-based model which recorded the best accuracy values. In addition, the new system supersedes the existing models because it was experimentally validated with real-world customer data. This experimental validation of the new model showcased how reliable the model is in a real-world energy theft scenario.

5. CONCLUSION

The work on the developing and implementing an artificial intelligence (AI) driven system for electricity theft detection is aimed to develop a system that can automatically identify and detect instances of electricity theft in real time. It has been observed that while AI and SVM algorithm is a popular algorithm for solving regression and classification problems, issues of optimal hyper-parameter selection to facilitate the best hyper-plane decision boundary has remained a major challenge. To solve this problem, optimization algorithm was applied to train SVM. The system result considering FDR reported that 0.110 was achieved for the particle swarm based SVM model. When TPR was considered for analysis, it was observed that particle swarm based SVM attained a score of 0.89. In addition, particle swarm based SVM attained PPV of 0.895. In terms of accuracy, the particle swarm based SVM reported an accuracy of 0.857. Overall, the result showed that the particle swarm based SVM outperformed other counterpart models from the system validation achieved through comparative analysis, hence it is recommended for use to develop the new software for energy theft investigation. The study underscores the potential of AI technologies to revolutionized electricity theft detection.

6. RECOMMENDATION

Based on the findings and outcomes of this study, several recommendations are proposed to further enhance the development and deployment of AI-driven systems for electricity theft detection, but the most important among them is continuous model training and updating**.** The nature of electricity theft is dynamic, with perpetrators continuously devising new methods to bypass detection. Therefore, it is crucial to implement a framework for continuous model training and updating. Regularly updating the AI models with new data will ensure that the system remains effective against emerging theft techniques.

REFERENCES

[1] Gbenga, Y. (2023). The crime of electricity theft and punishment for offenders. Retrieved from https://tribuneonlineng.com/the-crime-of-electricity-theft-and-punishment-for-offenders/

[2] Gbolahan, O. O. (2017). Electricity theft and power quality in Nigeria. International Journal of Engineering Research & Technology (IJERT), 6(6), 1180-.1184.

[3] Ebole, A. F. (2020). Electricity power theft detection using wireless prepaid meter. *International Journal of Computer Science and Information Security (IJCSIS), 18*(5), 36-78. http://sites.google.com/site/ijcsis/

[4] Glauner, P. (2019). Artificial intelligence for the detection of electricity theft and irregular power usage in emerging markets. Doctoral dissertation. University of Luxembourg.

[5] Javaid, P., Almogren, A., Adil, M., Javed, M., & Zuair, M. (2022). RFE based feature selection and KNNOR based data balancing for electricity theft detection using BiLSTM-LogitBoost stacking ensemble model. IEEE Access, 10, 112948-112963. https://doi.org/10.1109/ACCESS.2022.3215532

[6] Mhaske, D., Satam, R., Londhe, S., Kohad, T., & Kadam, S. (2022). An efficient electricity theft detection using XGBoost. *International Journal of Engineering Applied Sciences and Technology*, *6*(10), 282-287.

[7] Onibonoje, M. (2021). An IoT design approach to residual energy metering, billing, and protection. 2021 IEEE International IoT, Electronics, and Mechatronics Conference (EMTRONICS). 614-617 https://doi.org/10.1109/IEMTRONICS52119.2021.9422580

[8] Reshma, R., Suryalakshmi, S., Josephin, S., Athira, A., & Sruthy, E. (2022). Electricity theft detection using machine learning. International Journal of Engineering Research & Technology (IJERT), 10(4), 101-104.

[9] Bohani, F., Suliman, A., Saripuddin, M., Sameon, S., Salleh, S., & Nazeri, S. (2021). A comprehensive analysis of supervised learning techniques for electricity theft detection. Journal of Electrical and Computer Engineering, Article ID 9136206. https://doi.org/10.1155/2021/9136206

[10] Nwobodo-Nzeribe, H. N., Ozoemena, P. C., & Odo. (2022). Modeling of an intelligent cooking gas leakage detection system using convolutional neural network. *American Journal of Applied Sciences and Engineering*, *3*(5), 13-23.

[11] Tyryshkina, Y., & Tumkovskiy, S. (2022). Method for accelerating the joining of distributed datasets by a given criterion. *Journal of Automation and Information Sciences*, *54*(5), 2-11. https://doi.org/10.31799/1684-8853-2022-5-2-11

[12] Johnson, R. E., Grove, A., & Clarke, A. (2019). Pillar integration process: A joint display technique to integrate data in mixed methods research. *Journal of Mixed Methods Research*, 13(3), 301-320.

[13] Mengash H, Lal Hussain, Hany Mahgoub, A. Al-Qarafi, Mohamed K. Nour, Radwa Marzouk, S. A. Qureshi, & A. Hilal. (2022). Smart Cities-Based Improving Atmospheric Particulate Matters Prediction Using Chi-Square Feature Selection Methods by Employing Machine Learning Techniques. *Applied Artificial Intelligence*, 36(4), 303-324.

[14] Assegie, T. A., Tulasi, R., & Elanangai, V. (2022). Exploring the performance of feature selection method using breast cancer dataset. International Journal of Electrical and Computer Engineering (IJECE), 25(1), 232-237. https://doi.org/10.11591/ijeecs.v25.i1.pp232-237

[15] Goyal, N., Vempala, S., & Xiao, Y. (2013). Fourier PCA and robust tensor decomposition. Proceedings of the 46th Annual ACM Symposium on Theory of Computing, 46(1), 584-593. https://doi.org/10.1145/2591796.2591875

[16] Basna, S. H., & Abdulazeez, A. (2021). A review of principal component analysis algorithm for dimensionality reduction. Journal of Soft Computing and Decision Support Systems, 2(1), 3-10. https://doi.org/10.30880/JSCDM.2021.02.01.003

[17] Wang, D., Tan, D., & Liu, L. (2018). Particle swarm optimization algorithm: An overview. Soft Computing, 22(2), 387-408. https://doi.org/10.1007/s00500-016-2474-6

[18] Chen, Y., Hua, G., Feng, D., Zang, H., Wei, Z., & Sun, G. (2020). Electricity theft detection model for smart meter based on residual neural network. *IEEE Access*, *8*, 182651-182664. https://doi.org/10.1109/ACCESS.2020.3026441

[19] Liu, Y., Zeng, Z., & Dong, S. (2020). FPETD: Fault-tolerant and privacy-preserving electricity theft detection. *IEEE Transactions on Smart Grid*, *12*(1), 745-756. https://doi.org/10.1109/TSG.2020.3021518

[20] Madhure, R., Raman, R., & Singh, S. (2020). CNN-LSTM Based Electricity Theft Detector in Advanced Metering Infrastructure. *2020 IEEE International Conference on Computing, Power, and Communication Technologies (GUCON)*, 845-850. https://doi.org/10.1109/GUCON48875.2020.9231172.

[21] Ullah, A., Javaid, N., Yahaya, A., Sultana, T., Al-Zahrani, F., & Zaman, F. (2021). A hybrid deep neural network for electricity theft detection using intelligent antenna-based smart meters. Wireless Communications and Mobile Computing, Article ID 9933111. https://doi.org/10.1155/2021/9933111

[22] Ayub, N., Aurangzeb, K., Awais, M., & Ali, U. (2020). Electricity theft detection using CNN-GRU and manta ray foraging optimization algorithm. 2020 IEEE 23rd International Multitopic Conference (INMIC), 1-6. https://doi.org/10.1109/INMIC50486.2020.9318196

[23] Syed, D., Abu-Rub, H., Refaat, S., & Xie, L. (2020). Detection of energy theft in smart grids using electricity consumption patterns. 2020 IEEE International Conference on Big Data (Big Data) 4059-4063. https://doi.org/10.1109/BigData50022.2020.9378190

[24] Nabil, M., Ismail, M., Mahmoud, M., Shahin, M., Qaraqe, K., & Serpedin, E. (2018). Deep recurrent electricity theft detection in AMI networks with random tuning of hyper-parameters. 2018 24th International Conference on Pattern Recognition (ICPR) 740-745. https://doi.org/10.1109/ICPR.2018.8545788.