# MACHINE LEARNING FOR ANOMALY DETECTION IN SMART GRID ENERGY CONSUMPTION: A ONE-CLASS SVM APPROACH

[1]Agbo, E. R., [1]Olajide, I. A., [1]Itodo, E. S., [2]Faleye, O. P.

*[1]Department of Electrical and Electronics Engineering, Federal University of Technology, Akure, Nigeria*
*[2]Department of Electrical, Electronics and Computer Engineering, Afe Babalola University, Ado-Ekiti, Nigeria*

**Correspondence: iaadebanjo@futa.edu.ng*

Agbo, E. R., Olajide, I. A., Itodo, E. S., Faleye, O. P. (2025): Machine Learning for Anomaly Detection in Smart Grid Energy Consumption: A One-Class SVM Approach. *FUTA Journal of Engineering and Engineering Technology / 19(1), 208-215*

**Received Date: 10.5.25** **Accepted Date: 10.6.25**

***Abstract***
Energy monitoring holds significant implications for sustainability, cost-efficiency, and energy security in Energy usage. In this paper, the One-Class Support Vector Machine model (OCSVM) was employed to monitor energy usage. The system collected real-time data on voltage, current, power, and other energy parameters from a residential apartment over one month. Advanced data analytics provided useful information into consumption patterns. The OCSVM model was trained to identify anomalies indicative of potential energy/electricity theft. The implemented system effectively acquired real-time electrical data, enabling analysis of peak usage times, recurring trends, and parameter correlations. The trained OCSVM model exhibited a precision of 0.9525, recall of 0.9441, and F1 score of 0.948 in detecting energy consumption anomalies, thereby demonstrating its effectiveness in energy theft detection.

***Keywords:*** *Energy monitoring, energy meter, energy theft detection, one-class support Vector machine*

## Introduction

The growing demand for energy and increasing environmental concerns have heightened the need for optimized energy consumption and anomaly detection, such as energy theft (Yip et al., 2018; Fang et al., 2020). Electricity providers and distributors have constantly made efforts to make energy accessible to customers but there are still losses incurred in technical and non-technical forms. Figure 1 gives the classification and types of Electric power losses. Technical Losses (TL) arise as a result of grid failure, power outages and short circuits (Fang et al., 2020), while Non-Technical Losses (NTL) are caused by consumer inappropriate energy usage and connection, theft etc. (Guerrero et al., 2017). Energy Theft is the use of electricity from electricity providers or utility companies without a legitimate access or legal binding (Ahmad et al., 2017), and it means that the energy consumed is invariably not billed (Aldegheishem et al., 2021). Energy/Electricity theft is a prevalent situation in both the developing and developed nations, which has made energy monitoring and theft detection a necessity.

Energy theft causes increase in energy demand, substantial energy income loss, huge energy load on existing distribution networks (Aldegheishem et al., 2021; Mahmood et al., 2015). Aside these effects, the brunt of the energy thefts outcome is bore by consumers who are rightly connected by paying the extra bills incurred by the disloyal consumers (Ahmad et al., 2017; Ramos et al., 2016). In Nigeria, according to (Shokoya and Raji, 2019), the Electricity Distribution Companies (Discos) loses about ₦30 billion monthly to energy theft. Energy theft is considered to be responsible for about 80% of energy losses in Nigeria (David et al., 2017). Conversely, energy theft poses a significant worldwide problem that negatively affects utility companies and electricity users. In the US, it was reported that about $6 billion is lost annually due to energy theft, while about 20% of the generated power in India is lost to energy theft (Razavi and Fleury, 2019). According to Zulu and Dzobo (2023), Energy theft poses substantial financial challenges for utilities, with global losses estimated at over $25 billion annually. It disrupts distribution networks, causes equipment stress and presents safety hazards. Societal impacts include perpetuating inequalities in reliable power access.

Energy theft spans across developed and underdeveloped countries of the world, thereby

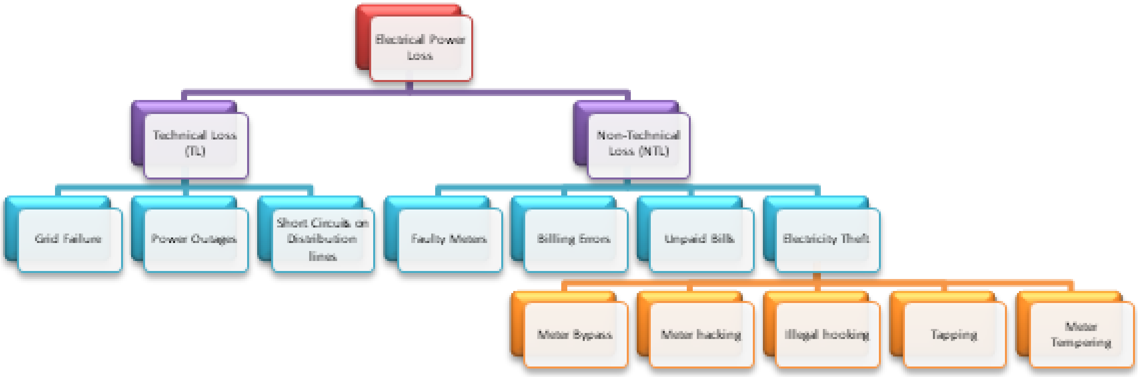


**Figure 1**: Electric Power Loss Classification (Aldegheishem et al., 2021)

simply being a global issue of concern for providers and distributors of electricity. The extent of the economic impact of energy theft calls for different approaches to curb or reduce its effect on the economy; with energy monitoring being one of such approaches. Therefore, energy monitoring systems play a crucial role in tracking, recording, and analyzing energy consumption. Energy monitoring enables energy conservation, efficiency, and cost savings (Al-Ali et al., 2017).

Energy has been monitored for several years using the traditional method of physical inspection which is not efficient and effective due to human errors. In order to address the rising issues and effects brought about by energy theft, various options have been developed. There has been a significant amount of research in energy monitoring and detection over the years since the traditional method of physical inspection has not produced the desired results. Energy scientists and specialists have adopted machine learning and the study of obtained data from the Smart Grid (SG) (Ahmad et al., 2022). The study presented in this paper implemented an energy monitoring system integrated with machine learning model based on the One-Class Support Vector Machine (OCSVM) algorithm. The integration of advanced machine learning techniques, such as OCSVM, holds promise for detecting and mitigating energy theft.

### One-Class Support Vector Machines (OCSVM) for Anomaly Detection

OCSVM is an unsupervised machine learning technique used for outlier detection by estimating the boundary separating data from the origin in high-dimensional space (Hodge and Austin, 2004). It has been applied to detect anomalies like network intrusions, fraud and defective images.

### The kernel trick of OCSVM

The brilliance of the kernel lies in its application of the "kernel trick." Instead of explicitly transforming the data into a higher-dimensional space, the kernel computes the similarity in that space without calculating the new coordinates. It allows computation in the higher-dimensional space without explicitly transforming the data and also avoids the computational burden associated with high-dimensional transformations, making OCSVM computationally efficient even in non-linear scenarios. Various kernel functions like linear, polynomial and Radial Basis Function (RBF) cater to data characteristics. In Support Vector Machine (SVM), the decision function is often used and it is expressed as shown in Equation 1 (Cortes and Vapnik, 1995).

$$\boldsymbol{f(x) = sin\sum_{i=1}^{N}(\alpha_i y_i K(x_i, x) + b)} \qquad \textbf{(1)}$$

where $\boldsymbol{f(x)}$ is the decision or prediction function, $\boldsymbol{x}$ is the feature vector, *N* is the total number of training samples, $\boldsymbol{a_i}$ and $\boldsymbol{y_i}$ are Lagrange multipliers and class labels of training samples, $\boldsymbol{K(x_i, x)}$ is the kernel function, $\boldsymbol{x_i}$ is the *i-th* training sample's feature vector, and $\boldsymbol{b}$ is the bias term or intercept

Real-world situations are rarely linear, and complex, non-linear interactions are frequently seen in datasets (Genzel and Kutyniok, 2016). The kernel trick is the main attraction here. The kernel technique indirectly translates the input space into a higher-dimensional feature space rather than trying to change the data directly (Campbell, 2001). A kernel function (such as a polynomial or radial basis function) that computes the similarity between data points in the higher-dimensional space without explicitly computing the new coordinates facilitates this transition (Saini, 2023).

Several types of kernels are employed in SVM, each catering to specific characteristics of datasets. **Linear Kernel** is the simplest, representing the inner product between feature vectors. It is efficient for datasets where classes can be effectively separated by a straight line, as observed in Equation 2 as,

$$K(x_i, x_j) = x_i . x_j \qquad (2)$$

where $x_i$ is the i-th feature vector, and $x_j$ is the j-th feature vector

**Polynomial Kernel** captures non-linear relationships by introducing polynomial terms (Cao, 2011). The degree of the polynomial *d* is a parameter that can be tuned based on the complexity of the dataset. Therefore, Equation 2 becomes Equation 3 as shown;

$$K(x_i, x_j) = (x_i . x_j + 1)^d \qquad (3)$$

where *d* is the polynomial's degree.

The **Radial Basis Function (RBF) or Gaussian Kernel** is widely used for its ability to handle complex, non-linear relationships (Razaque, 2021) and it is expressed in equation 4. It is characterized by a smooth, bell-shaped curve and is particularly effective in scenarios where the decision boundaries are intricate as shown in Equation 4 (Ghosh and Nag, 2001).

$$K(x_i, x_j) = exp\left(-\frac{\|x_i - x_j\|^2}{2\sigma^2}\right) \qquad (4)$$

where $\|x_i - x_j\|^2$ is the euclidean distance between two feature vectors, $x_i$ and $x_j$, $\boldsymbol{\sigma}$ is a parameter controlling the width of the Gaussian.

This study presents the design, implementation, and evaluation of an energy monitoring system capable of real-time data acquisition and theft detection using the OCSVM model. The system's performance was assessed through real-time data acquisition, electrical data analysis, and the accuracy of the OCSVM model in identifying energy consumption anomalies.

## Methodology

### System Design and Implementation

The energy monitoring system was designed to measure and record critical electrical parameters, including voltage, current, power factor, and power. The block diagram of the design is shown in Figure 2. The system comprised of an Arduino UNO microcontroller, a PZEM-004T module for electrical parameter measurement, an SD card module for data logging, an I2C LCD screen for real-time data visualization, and other supporting components.

The system architecture involved sensor integration, real-time data collection and transmission, and advanced data analysis. The Arduino UNO served as the central processing unit, interfacing with the PZEM-004T module to acquire electrical data and communicating with the SD card module for data storage and the LCD screen for data visualization.

### Data Collection and Analysis

Data collection was conducted over a comprehensive one-month period with one hour interval in a selected residential apartment. The system continuously recorded voltage, current, power factor, and power data, capturing a spectrum of usage patterns. Advanced data analytics techniques were employed to process and analyze the collected data. Descriptive statistics, including mean, median, and mode, were computed to understand central tendencies and variations in energy consumption. Time series analysis identified peak usage times, recurring trends, and seasonality patterns in the data gathered. Correlation analysis explored relationships between various electrical

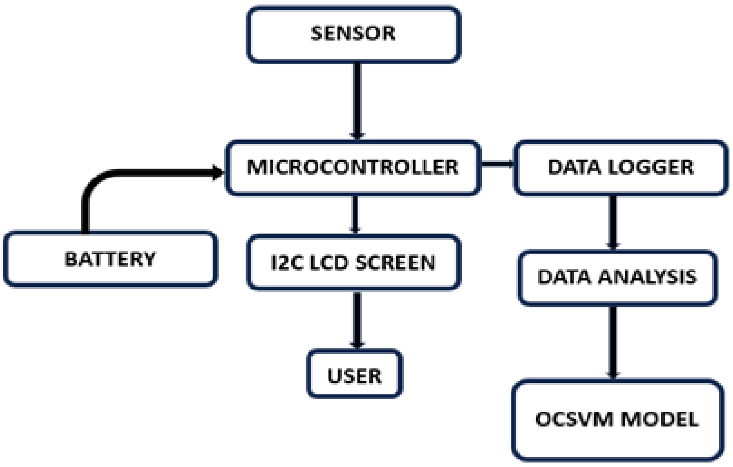


**Figure 2**: Block diagram of the system

parameters, contributing to a comprehensive understanding of energy consumption dynamics.

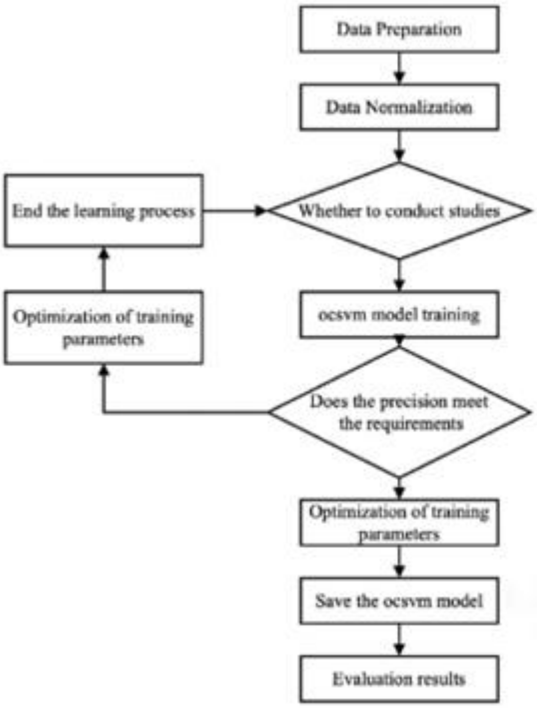

Data Preparation
Data Normalization
Whether to conduct studies
End the learning process
ocsvm model training
Optimization of training parameters
Does the precision meet the requirements
Optimization of training parameters
Save the ocsvm model
Evaluation results

**Figure 3**: OCSVM model algorithm flow chart

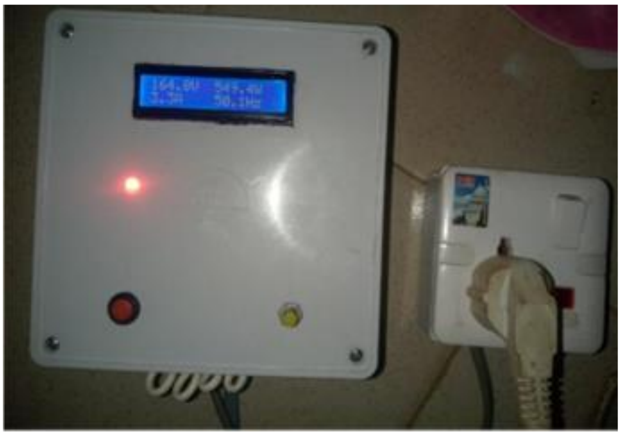


**Figure 4**: Energy monitoring system during test

**OCSVM Model Development and Training**

The OCSVM algorithm was chosen for its ability to detect anomalies in energy consumption patterns, indicating potential energy theft. The model was trained using a labeled dataset consisting of normal and anomalous instances of energy consumption. The flowchart of the model development and training path is provided in Figure 3. Feature selection involved identifying relevant electrical parameters, such as voltage, current, power factor, and power, as input features for the model. Hyperparameter tuning was performed to optimize the model's performance, including the kernel type, nu, and gamma parameters.

The training process involved separating the dataset into training and testing subsets. The OCSVM model was trained on the training data, learning the characteristics of normal energy consumption patterns. Subsequently, the model's performance was evaluated on the test data using metrics such as precision, recall, F1 score, and confusion matrix.

**Results and Discussion**

**Performance of the Energy Monitoring System**

The implemented energy monitoring system demonstrated commendable effectiveness in real-time data acquisition. The energy monitoring system under test is shown in Figure 4. It seamlessly recorded voltage, current, frequency, power, and power factor, providing a comprehensive snapshot of the electrical behaviour within the monitored environment.

## Electrical Data Analysis

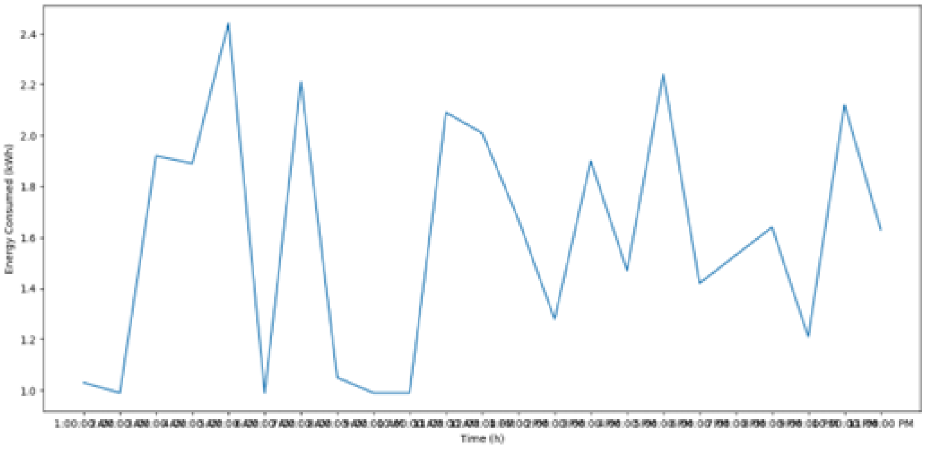
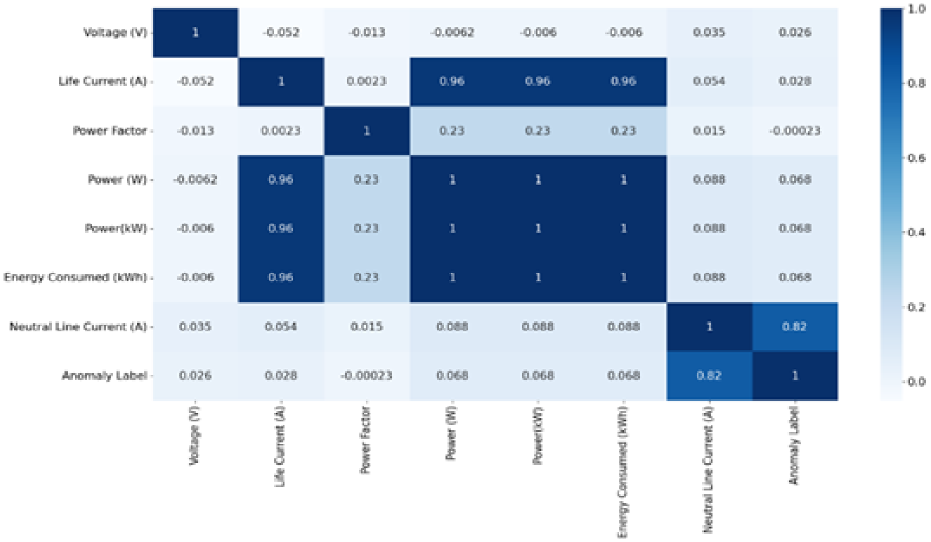


**Figure 5**: Energy consumption pattern of one of the days



| | Voltage (V) | Life Current (A) | Power Factor | Power (W) | Power(kW) | Energy Consumed (kWh) | Neutral Line Current (A) | Anomaly Label |
|---|---|---|---|---|---|---|---|---|
| Voltage (V) | 1 | -0.052 | -0.013 | -0.0062 | -0.006 | -0.006 | 0.035 | 0.026 |
| Life Current (A) | -0.052 | 1 | 0.0023 | 0.96 | 0.96 | 0.96 | 0.054 | 0.028 |
| Power Factor | -0.013 | 0.0023 | 1 | 0.23 | 0.23 | 0.23 | 0.015 | -0.00023 |
| Power (W) | -0.0062 | 0.96 | 0.23 | 1 | 1 | 1 | 0.088 | 0.068 |
| Power(kW) | -0.006 | 0.96 | 0.23 | 1 | 1 | 1 | 0.088 | 0.068 |
| Energy Consumed (kWh) | -0.006 | 0.96 | 0.23 | 1 | 1 | 1 | 0.088 | 0.068 |
| Neutral Line Current (A) | 0.035 | 0.054 | 0.015 | 0.088 | 0.088 | 0.088 | 1 | 0.82 |
| Anomaly Label | 0.026 | 0.028 | -0.00023 | 0.068 | 0.068 | 0.068 | 0.82 | 1 |

**Figure 6**: Correlation among the electrical parameters

The analysis of the acquired energy consumption data revealed valuable information into patterns and correlations between various electrical parameters.

1. Peak Usage Times: By analyzing the recorded values over different time intervals, the system effectively identified periods of heightened energy demand, aiding in optimization and load management. The trend of usage of energy is provided for One (1) day in Figure 5.

2. Recurring Trends: The systematic analysis unveiled recurring daily, weekly, or seasonal trends in energy consumption, facilitating proactive measures for energy conservation.

3. Correlation Analysis: Exploring the relationships among voltage, current, frequency, power, power factor, and energy consumed contributed to a comprehensive understanding of the energy system's dynamics and overall efficiency. The correlation heatmap is presented in Figure 6. It can be observed that the electrical parameters were well correlated with the diagonal values of 1.

## One-Class Support Vector Machine (OCSVM) Model Results

The decision boundary for the One-Class Support Vector Machine (OCSVM) on how it separates data is shown in Figure 7. Each data point is represented by 'x', The red shaded area represents the normal region as learned by the OCSVM. Any new data point falling within this red area would be classified by the OCSVM as "normal" or "expected" behavior. The OCSVM has learned a complex, non-linear boundary to encompass the majority of the black 'x' points. The blue region represents the anomaly region. Any new data point that falls into this blue area would be classified by the OCSVM as an anomaly.

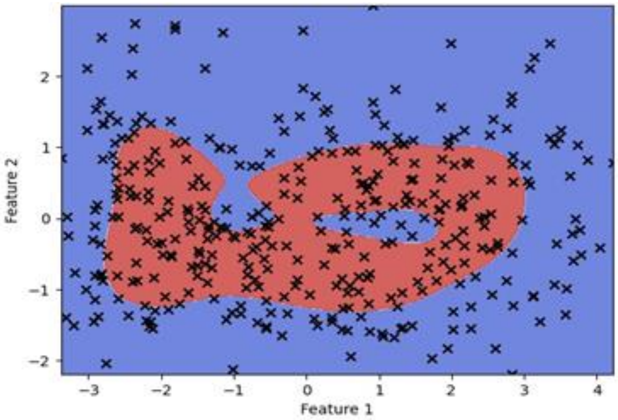


**Figure 7**: Decision boundary of the One-Class Support Vector Machine (OCSVM)

**Table 1**: The obtained performance matrices

| S/N | PARAMETER | RESULT |
|---|---|---|
| 1 | Precision score | 0.9525 |
| 2 | Recall score | 0.9441 |
| 3 | $F_1$ score | 0.948 |

The trained OCSVM model exhibited significant strength in identifying anomalous patterns suggestive of potential energy theft. Key performance metrics used are:

**Precision Score:** 0.9525, indicating that approximately 95.25% of instances flagged as anomalies were true anomalies.

**Recall Score:** 0.9441, implying that the model correctly identified 94.41% of actual anomaly cases.

**F1 Score:** 0.948, demonstrating a robust balance between precision and recall.

The confusion matrix further illustrated the model's ability to effectively differentiate between normal and anomalous energy consumption instances. Overall, these results demonstrate the OCSVM model's effectiveness in detecting energy consumption anomalies, facilitating electricity theft detection within residential settings.

## Conclusion

This study successfully implemented an energy monitoring system integrated with an OCSVM-based energy theft detection model. The system effectively acquired real-time electrical data, enabling analysis of energy consumption patterns, peak usage times, and parameter correlations. The trained OCSVM model exhibited high precision, recall, and F1 scores, indicating its ability to accurately identify anomalies indicative of potential energy theft. These findings contribute to enhancing energy efficiency and security in residential apartments. Future research directions include expanding the system to three-phase AC systems, refining the anomaly detection model with additional training data and algorithms, building a centralized dashboard for data visualization and system control, and conducting field trials across diverse residential facilities.

## References

Ahmad, T., Chen, H., Wang, J. and Guo, Y. (2018). Review of various modeling techniques for the detection of electricity theft in smart grid environment. Renewable and Sustainable Energy Reviews, 82, 2916-2933.

Ahmad, T., Madonski, R., Zhang, D., Huang, C. and Mujeeb, A. (2022). Data-driven probabilistic machine learning in sustainable smart energy/smart energy systems: Key developments, challenges, and future research opportunities in the context of smart grid paradigm. Renewable and Sustainable Energy Reviews, 160,1-35.

Al-Ali, A.R., Zualkernan, I.A., Rashid, M., Gupta, R. and AliKarar, M. (2017). A smart home energy management system using IoT and big data analytics approach. IEEE Transactions on Consumer Electronics, 63(4), 426-434.

Aldegheishem, A., Anwar, M., Javaid, N., Alrajeh, N., Shafiq, M., and Ahmed, H. (2021). Towards sustainable energy efficiency with intelligent electricity theft detection in smart grids emphasising enhanced neural networks. IEEE Access, 9, 25036-25061.

Campbell, C. (2001). An introduction to kernel methods. Studies in Fuzziness and Soft Computing, 66, 155-192.

Cao, D. S., Liang, Y. Z., Xu, Q. S., Hu, Q. N., Zhang, L. X. and Fu, G. H. (2011). Exploring nonlinear relationships in chemical data using kernel-based methods. Chemometrics and Intelligent Laboratory Systems, 107(1), 106-115.

Cortes, C. and Vapnik, V. (1995). Support-Vector Networks. Machine Learning, 20(3), 273-297.

David, F. C., James, A. C., and Onyinye, A. H. (2017) Controlling Electricity Theft, A Smart Meter Approach: Case Study Nigeria, 1-17

Feng, L., Xu, S., Zhang, L., Wu, J., Zhang, J., Chu, C. and Shi, H. (2020). Anomaly detection for electricity consumption in cloud computing: framework, methods, applications, and challenges. EURASIP Journal on Wireless Communications and Networking, 1, 194, 1-12.

Genzel, M. and Kutyniok, G. (2016). A mathematical framework for feature selection from real-world data with non-linear observations. arXiv preprint arXiv:1608.08852, 1-36.

Ghosh, J. and Nag, A. (2001). An overview of radial basis function networks. Radial basis function networks 2: new advances in design, 1-36.

Guerrero, J. I., Monedero, I., Biscarri, F., Biscarri, J., Millan, R. and Leon, C. (2017). Non-technical losses reduction by improving the inspections accuracy in a power utility. IEEE Transactions on Power Systems, 33(2), 1209-1218.

Hodge, V., and Austin, J. (2004). A survey of outlier detection methodologies. Artificial intelligence review, 22, 85-126

Mahmood, A., Javaid, N., Khan, M. A. and Razzaq, S. (2015). An overview of load management techniques in smart grid. International Journal of Energy Research, 39(11), 1437-1450.

Ramos, C. C., Rodrigues, D., de Souza, A. N. and Papa, J. P. (2016). On the study of commercial losses in Brazil: A binary black hole algorithm for theft characterization. IEEE Transactions on Smart Grid, 9(2), 676-683.

Razaque, A., Ben Haj Frej, M., Almi'ani, M., Alotaibi, M. and Alotaibi, B. (2021). Improved support vector machine enabled radial basis function and linear variants for remote sensing image classification. Sensors, 21(13), 1-26.

Razavi, R. and Fleury, M. (2019). Socio-economic predictors of electricity theft in developing countries: An Indian case study. Energy for Sustainable Development, 49, 1-10.

Saini, A. (2023). Guide on Support Vector Machine (SVM) Algorithm. Retrieved from Analytics Vidhya: https://www.analyticsvidhya.com/blog/2021/10/support-vector-machinessvm-a-complete-guide-for-beginners/, June 20, 2024

Shokoya, N. O. and Raji, A. K. (2019). Electricity theft mitigation in the Nigerian power sector. International Journal of Engineering and Technology, 8(4), 467-472.

Yip, S. C., Tan, W. N., Tan, C., Gan, M. T. and Wong, K. (2018). An anomaly detection framework for identifying energy theft and defective meters in smart grids. International Journal of Electrical Power & Energy Systems, 101, 189-203.

Zulu, C. L. and Dzobo, O. (2023). Real-time power theft monitoring and detection system with double connected data capture system. Electrical Engineering, 105(5), 3065–3083.