International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V74I1P117

Volume 74 Issue 1, 227-235, January 2026

Original Article

Comparative Analysis of Energy Theft Detection in a Power System using Support Vector Machine and Quantitative Technique

Olushola Akintola[1], Babatunde Adetokun[2], Oghenewvogaga Oghorada[3]

[1,2,3]*Electrical and Electronics Engineering, Nile University of Nigeria, Abuja, Nigeria.*

[1]*Corresponding Author : sholakintola@gmail.com*

Received: 28 October 2025 Revised: 29 December 2025 Accepted: 06 January 2026 Published: 14 January 2026

Abstract *- This study compares energy theft detection methods using qualitative analysis techniques and a Support Vector Machine (SVM) model. With a precision of 97.86%, a recall of 99.93%, an F1-score of 98.88%, and an accuracy of 97.94%, the findings show that SVM performed well across all key evaluation metrics. However, qualitative analysis revealed an average consistency of 80% across these indicators, indicating a higher risk of misclassification and lower reliability. The results demonstrate that, compared to traditional qualitative methods, SVM provides better detection accuracy, reduces false alarms, and ensures comprehensive identification of theft cases. When compared to other related works on an overall basis, the results were superior. These findings highlight the potential of machine learning models, particularly SVM, as a scalable and dependable approach to preventing electricity theft in modern power grids.*

Keywords *- Distribution systems, Energy theft detections, Non-technical losses, Support Vector Machine, Quantitative analysis.*

1. Introduction

A stable power system is essential to the social well-being and economic development of modern countries [1]. Nonetheless, one of the most significant issues utilities face worldwide is electricity theft. This concept, among other things, increases technical losses, degrades the supply, reduces efficiency, and results in large revenue losses. Energy theft is estimated to cost a significant amount of money annually, with developing countries being disproportionately affected due to inadequate monitoring, insufficient enforcement, and underdeveloped technological infrastructure [2].

To mitigate these issues, researchers have developed several methods for detecting power system theft. Traditional methods, such as meter audits and physical inspections, take a lot of time and often fail to identify sophisticated energy-stealing strategies [3]. Advances in digital metering, communication networks, and data analytics have enabled more intelligent, automated, and efficient detection techniques. Advanced Metering Infrastructure (AMI), machine learning algorithms, data-driven anomaly detection systems, and smart meters have shown great potential in identifying unusual usage patterns and more accurately discovering theft. Additionally, cutting-edge strategies for avoiding electricity theft include Internet of Things (IoT)-based monitoring systems, wireless sensor networks, and blockchain for secure transactions [4]. Despite a number of mitigation strategies, including smart metering, supervisory control systems, and regulatory enforcement, energy theft detection and prevention remain inadequate [5]. Traditional statistical approaches and rule-based methods often fail to cope with the complexity of consumer behavior, evolving theft techniques, and the large volume of consumption data in modern grids [6].

This work presents a comparative analysis of the energy theft detection using Support Vector Machine (SVM) and Quantitative analysis.

2. Literature Review

Energy theft, a major component of Non-Technical Losses (NTLs), continues to undermine the operational efficiency, financial viability, and long-term sustainability of electricity distribution networks. With the rapid penetration of smart meters and Advanced Metering Infrastructures (AMI), recent research has shifted towards data-driven and intelligent analytics for detecting anomalies in consumption patterns. This section synthesizes contemporary literature, connecting methodologies, findings, and limitations to reveal the evolving landscape of energy theft detection and highlight critical research gaps. By contrasting statistical indicators, Artificial Neural Networks (ANN), Adaptive Neuro-Fuzzy Inference Systems (ANFIS), and clustering approaches like k-means,

the work by [7] offered a thorough evaluation of AI techniques utilized in distribution networks. The analysis showed that AI methods outperformed traditional statistical guidelines. Similarly, [8] used an AI-powered method to identify electricity theft in a Nigerian distribution network. Despite these encouraging findings, it may be less generalizable to restrict the model to client recharge patterns rather than whole consumption profiles.

Also, [9] suggested a Denoising Diffusion Probabilistic Model (DDPM)-based ensemble method that reconstructed baseline consumption to detect irregularities. By combining reconstruction-based anomaly detection with forecasting error metrics, their ensemble method improved detection performance, particularly for stealthy and intermittent theft behaviors. In a related development, the study by [10] proposed a hybrid algorithm combining usage-pattern analysis and contextual features to detect non-technical losses in smart grids, demonstrating improved detection accuracy.

The study was found to lack generalized unsupervised solutions and large false positives across datasets. The work by [11] provided a global, holistic review of non-technical electricity losses, highlighting that large users often contribute more to losses. The study is largely conceptual and literature-based, lacking empirical case studies or quantitative modeling to assess the effectiveness of proposed interventions. Similarly, [12] presented a three-stage algorithm using smart meter data to estimate power and energy losses in distribution networks, combining topology recognition and load-flow analysis. The work was tested only on a small rural network.

A deep learning-based hybrid model for detecting electricity theft was carried out by [13], and it achieved good accuracy by tackling feature complexity and class imbalance. On the other hand, [14] suggested a hybrid Random Forest framework that improved anomaly detection and feature selection in smart-meter data. Both models require large, high-quality datasets and significant computational resources. An entropy-based metric that combines data from several sources to detect tampered or manipulated electrical meters was presented in [15]. The method showed good anomaly detection, although it could need rich, multi-source data. Also, a context-aware and pattern-based approach to detecting electricity theft is presented in [16]. The study by [17] proposed an AI-based model using real distribution-grid data enriched with engineered statistical and temporal features. The findings highlight the importance of combining raw consumption with temporal and contextual features to improve theft detection. Despite improved accuracy, collecting extensive feature sets is resource-intensive and difficult to implement in real-time.

Despite substantial progress in applying machine learning techniques to energy theft detection, several critical areas need to be addressed. Previous research has mostly concentrated on the use of certain algorithms without methodically contrasting how well they function under different data conditions. Furthermore, heuristic-based quantitative analysis is the foundation of contemporary methodologies; nevertheless, the integration of these quantitative techniques with machine learning classifiers has not been fully investigated.

2.1. Contribution of the Study

- The work provides a unique perspective on the efficacy of theft detection by integrating SVM with statistical and quantitative techniques.
- Using real-world consumer load profiles, the study assesses each method's accuracy, precision, recall, and computing efficiency.
- SVM provides robust classification capabilities for distinguishing normal and abnormal consumption patterns.
- The study offers recommendations for utilities to choose the best method for theft detection by comparing the two approaches.

The detection architecture for various approaches is shown in Section 2, and the methodology is shown in Section 3 of the remaining text. The results and comments are presented in Section 4, and the work is concluded in Section 5.

2.2. Detection Architecture for Different Approaches

The linkages between the different methods for detecting NTLs are established in this review. The techniques are categorized based on their detection mode and architecture. While AMI-based NAN approaches and hardware-based techniques are arranged under architecture-driven topologies, machine learning-based techniques are further divided into those that use sequential data, non-sequential data, and synthetic data. The general link between various detection techniques is shown in Figure 1 [18].

One of these five primary categories—synthetic data detection, sequential data detection, non-sequential data detection, neighborhood area networks, and IOT and hardware-based approaches—can be used to identify electricity theft.

2.2.1. Synthetic Data Detection

Synthetic data-based methods are becoming more and more popular in Electricity Theft Detection (ETD). This approach uses artificially created datasets to train and verify machine learning models. By simulating both normal (benign) and fraudulent (anomalous) customer behavior, synthetic datasets allow academics and utility suppliers to assess ETD models without depending on real consumption data. AI models are trained and tested using performance evaluation measures, including precision, recall, F1-score, and the AUC-ROC curve, once the data is generated and classified as either benign or fraudulent [18].

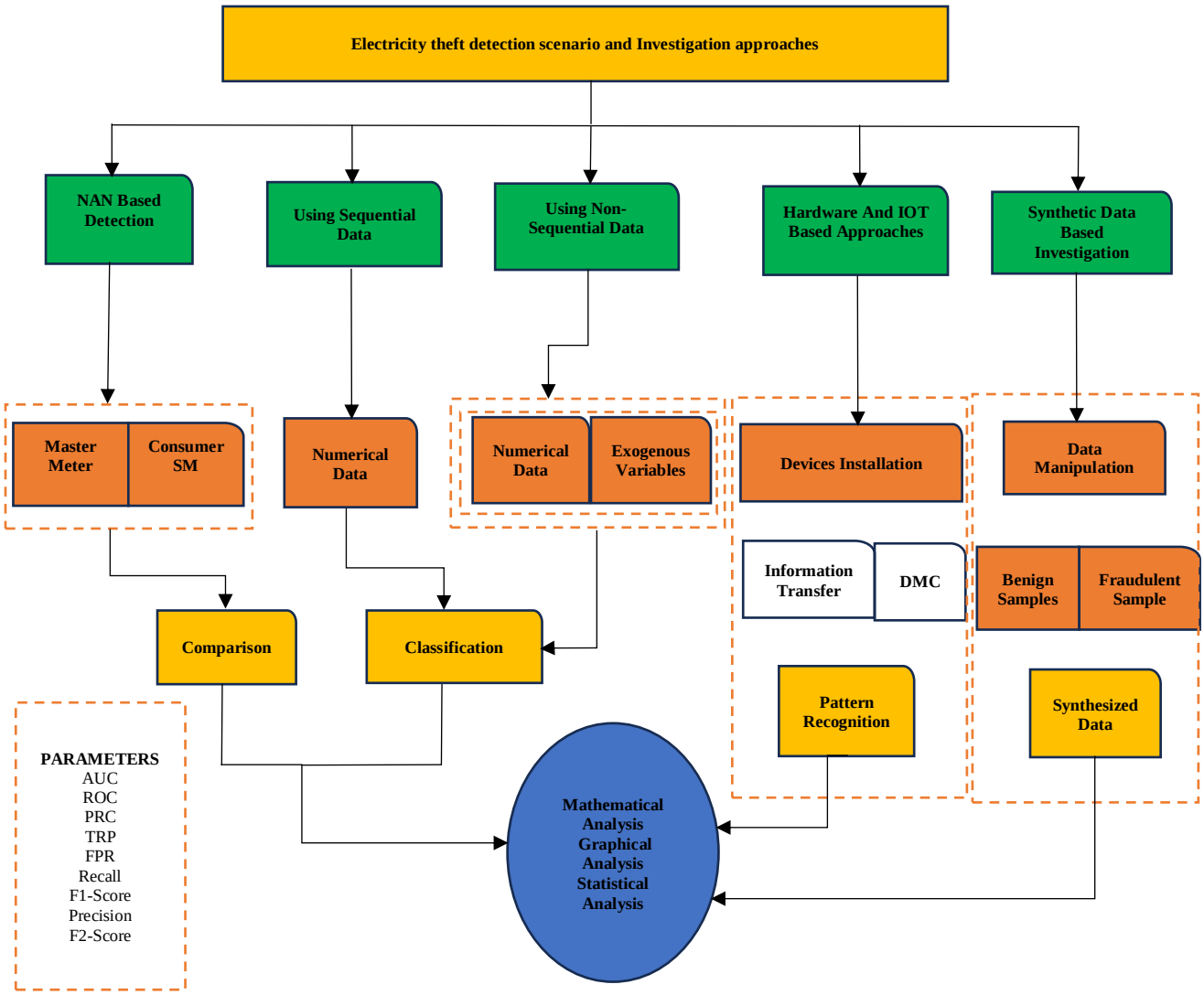

Fig. 1 Architecture of various detection scenarios [2]

2.2.2. Sequential Data Detection

Sequential data detection in ETD uses time-series analysis of power usage statistics to find anomalous patterns that can point to fraud. This technique separates anomalies from regular usage by using temporal correlations in the data. Since sequential data mostly consists of time-dependent features, Recurrent Neural Networks (RNNs) are widely employed to explain it. Following the required preprocessing, these RNN models are trained, and their efficacy is assessed using standard assessment criteria [19].

2.2.3. Non-Sequential Data Detection

Non-sequential data detection is the process of examining stationary or non-temporal data to identify anomalies that may indicate electricity theft. They primarily rely on time-series consumption patterns. This strategy focuses on features that are independent of the timing or sequence of data items. The process often begins with data gathering and preprocessing of non-temporal data, such as customer profiles, location data, payment history, and equipment features. Preprocessing standardizes category variables, corrects missing values, and transforms qualitative traits into quantitative formats suitable for analysis [20].

2.2.4. NAN-based Approaches

A Neighborhood Area Network (NAN) is composed of multiple customers connected to a local distribution network that is continuously monitored for irregularities. The Master Meter Method is a popular technique that measures the total energy provided to the NAN by installing a master meter on the low-voltage side of the distribution transformer. The aggregated consumption data gathered from each smart meter in the network is then compared by utilities with this reading.

A constant adjustment factor is added to the overall utilization to account for technical losses. Beyond this correction, any notable differences are seen as possible signs of non-technical losses, including electricity theft [21].

2.2.5. IoT and Hardware-Based Approaches

Two of the biggest NTL issues in power networks are meter tampering and electricity theft. Both hardware-based and Internet of Things (IoT)-enabled solutions have been developed to address these problems and improve detection. IoT techniques use networked sensors and gadgets to track energy consumption trends in real time. Microcontroller-equipped sensor nodes are positioned at strategic locations across the distribution network, such as customer connection points and the supply end of a distribution pole [22]. Hardware-based theft detection strategies focus on employing specialized devices to monitor and manage electricity usage in order to identify and prevent illegal consumption. One well-known example is the integration of smart metering systems with Advanced Metering Infrastructure (AMI). A significant advantage of hardware-based methods is their greater precision, which is achieved by direct measurement and control [23].

3. Materials and Methods

The proposed method employs a Support Vector Machine (SVM) classifier to identify electricity theft by analyzing customer consumption data collected from smart meters. The approach combines data preprocessing, feature extraction, and supervised learning to distinguish between legitimate energy usage and suspicious or fraudulent consumption patterns, as shown in Figure 2.

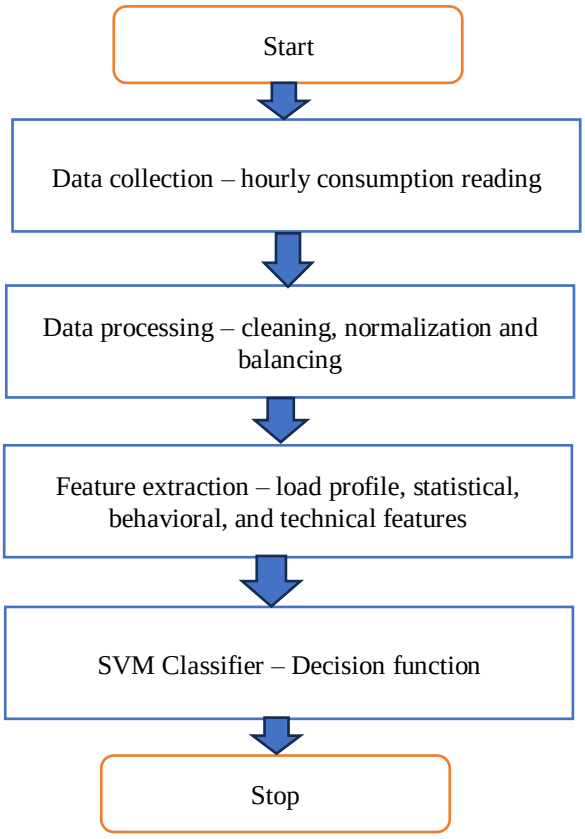

Fig. 2 Proposed method to detect the power theft using SVM

In Figure 2, the algorithm of machine learning begins with fetching the data from the data acquisition. Once the data is collected, it will go into the preprocessing. In this case, the data will be separated into test and training data. The trained data is the data that often appears or repeatedly appears during the data acquisition. The test data is different from the training data, plus some of the data behaves like trained data.

The trained data will go into the feature extraction, which uses many types of algorithms. This is important to confirm that the extracted data is the desired data. After the data has been extracted, it will be sent to the SVM algorithm for classification. Here, the trained data will mix with the tested data, and the SVM will group these two data types into a regression plot. Finally, the SVM will count the total number of data points, including those in the hyperplane, and hence produce +1 or -1 classification. The results of +1 and -1 will lead to the computation of accuracy, recall, precision, specificity, and F-measure as shown in Equations (1)- (4).

$$Accuracy = \frac{Number\ of\ correction\ predictions}{Total\ number\ of\ predictions\ made} \quad (1)$$

$$Precision = \frac{True\ positives}{True\ positives + False\ positives} \quad (2)$$

$$Recall = \frac{True\ positives}{True\ positives + False\ negatives} \quad (3)$$

$$F1\ Score = \frac{2 \times Precsion \times Recall}{Precision + Recall} \quad (4)$$

This paper presents the method of developing a system that can detect the illegal usage of electrical energy based on a 50 MVA distribution transformer in the substation. The 50 MVA distribution transformer is connected to 500 residents via a 1 kV bus, where most of the residents have active power loads instead of reactive power loads. There is an energy meter installed in the 50 MVA transformer to record the energy consumption by the total electrical loads.

The data collected from the energy meter is 5000 points. Among 5000 points of data, 2500 points are collected in the past three months, and the other 2500 points are current data points for about three months. Thus, the total months of collecting the data is 6 months. It is important to collect the past three months' data for comparison with the current three-month data. The characteristics of the data are the energy consumption in kWh. The data is then fed into the developed SVM algorithm for analysis on illegal use of energy.

The final analysis is the accuracy and precision of the data. To confirm the prediction is correct, the research uses a qualitative approach to collect the data from the engineer and technician who look after the 50 MVA transformer. The qualitative approach used is thematic analysis, where interviews are conducted to collect the data.

3.1. Data Collection

To collect the data, a 50 MVA transformer is selected with an energy meter installed. Figure 3 shows the 50 MVA transformer with an energy meter installed at the side. Such a transformer is a 115 kV to 38.5 kV step-down three-phase 50 Hz transformer.

Fig. 3 Energy meter built in the transformer to monitor total energy consumed by the consumers

The transformer is located in the substation and is connected to a bus bar, ready to distribute energy to more than 1,000 people. Under normal operation of the transformer, the energy consumption is approximately 50,000 kWh for a population of about 1,000. Since there is no development around the distribution area, the energy consumption remains below 50,000 kWh. On the other hand, if there is a sudden high energy consumption that occurs (meaning the energy usage is more than 5,000 kWh) for about three months continuously, and if there is no development around the area, then this might have two possibilities that cause high energy consumption. One is consumers installed with a high-power capacity of load, or consumers illegally using energy. Thus, the data collected will be grouped for analysis and classification as follows:

- Class 1 of data: no change of energy consumption or little change, which is not more than 50,000 kWh
- Class 2 of data: Change of 50,000 kWh energy consumption within a short time, but not more than one month
- Class 3 of data: A Change of 50,000 kWh energy consumption has occurred over more than 3 months, where the energy consumption is suddenly higher without seeing any new population increase or development around the area continuously
- Class 4 of data: Change of 50,000 kWh energy consumption happens more than 3 months, where the energy consumption is suddenly higher, with the evidence that a new population increase due to development has been found in the area.

Classes 1, 2, and 4 data refer to no normal data, where no illegal use of electricity was found. On the other hand, Class 4 data considers illegal use of data. Classes 1, 2, and 4 will be assigned as positive data, whereas Class 3 will be grouped as negative data. It may be skeptical about how to collect 5000 points of data in bulk.

The answer to this is to observe the energy consumption data changes every 10 minutes. Every 10 minutes, collect 100 data points of energy consumption. Thus, for 5,000 data points, it will take 500 minutes, which is 8.3 hours. The collection of the data does not necessarily have to be continuous, but it can take some gaps and continue for the next few minutes or the next day. As long as 8.3 hours are fulfilled, the data should be 5,000 points. If collecting the data is not continuous for 8.3 hours, that means the data collection is randomly chosen from time to time. The data collection will refer to one transformer with an energy meter installed on it.

Since this study employs MATLAB to develop the SVM algorithm, the dataset must be normalized before generating the regression function and plotting the results. The normalization process involves scaling down the high kWh values (dividing by 10,000) to obtain unitless data, enabling proper classification and visualization within the regression model. To validate the accuracy of the results, a qualitative approach is applied through interviews with local engineers regarding illegal electricity usage. The interview responses are then examined using thematic analysis, with the identified themes presented in Table 1.

Table 1. Thematic topics for the interview to collect the data to verify the data analyzed by the SVM

Theme 1: Awareness of illegal use of electricity	Theme 2: The significance of energy data changed	Theme 3: Overall electricity usage
This theme is proposed to collect information about awareness of illegal use of energy. The purpose of this theme is to find out whether, in the past or currently, the engineers have detected illegal use of electricity. The theme further explores how the engineers or electricity suppliers know someone has illegally used the energy.	This theme is to find out whether the fluctuation of meter readings will give significant information about the illegal use of energy. The theme also urges the responders to show how to identify illegal usage of energy from the fluctuation of meter readings.	This theme aims to know in general how the illegal use of energy reflects the energy suppliers and what the factors are that cause some consumers to use electricity illegally.

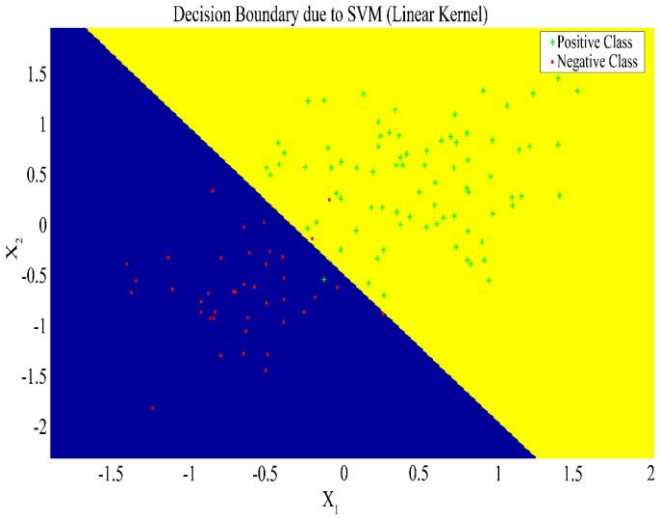

Fig. 4 Boundary of the regression plot

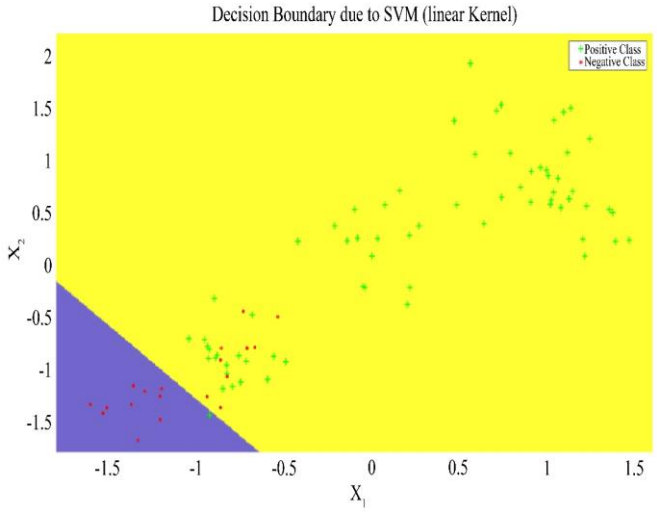

Fig. 5 Optimized boundary of the regression plot

4. Results and Discussion

4.1. Analysis and Decision Boundaries

Figures 4 and 5 show the decision boundary of the data before and after optimization. The decision boundary for the regression plot is to check the number of positive data points and negative data points that appear in the regression region. From the optimized results, the data is shifted to the right instead of being shifted down, as seen in Figure 5. After optimization, the positive data still have many in quantity compared to the negative data or FN. Note that the FN or negative data indicates a wrong result of interpretation by the classifier. The data does not mean that there is illegal use of energy in the region. According to the engineers in charge of the transformer, due to the large amount of energy values being recorded by the energy meter, if a small amount of energy is being illegally used, the system cannot detect it, or the meter cannot show it. For example, if the normal energy recorded is 1000 kWh, and if out of 1000 kWh, 0.5 kWh is being illegally used, then this 0.5 kWh is not significant because 1000 kWh >> 0.5 kWh. As a matter of fact, detecting energy theft at the distribution transformer can only detect large illegal energy usage by the users. Figure 6 illustrates the results of SVM processing the data versus the errors. As seen in Figure 6, when the iteration of the SVM increases to process the data, the magnitude of errors will decrease. The errors are due to the wrong interpretation of the energy data, and some of the data overlap or are repeated several times at the same time of detection. Because of that, the data has to be sent for a few iterations or training to reduce the error and remove the redundancy of the data. As can be seen in the results, when the instances are larger than 100, the iteration will stop and reduce the error to zero. Under this situation, the output of the data plotted in the regression will show less, and the data are significant for classifying whether there is a theft or not. The next section will show the computation of accuracy, F-score, recall, and precision from the optimized data.

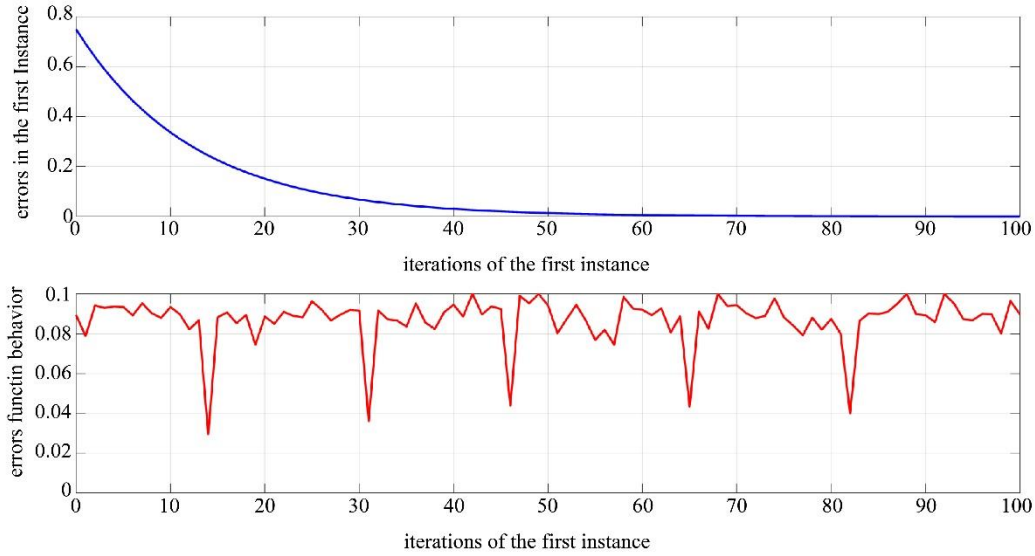

Fig. 6 SVM processing the data versus the errors

4.2. Analysis of the Overall Performance

Before computing the recall, F1-score, accuracy, and precision, it is important to describe the data set applied for the classification using SVM. Table 2 shows the description of the dataset before classification using SVM, while Figure 7 shows the confusion matrix results after SVM classification.

Table 2. Description of the dataset for classification

Description	Values
Temporal range of data	1 June 2024 - 31 December 2024
Dataset file size	10 MB (5000 data points)
A normal consumer consuming electricity	4573 (91.5%)
Customer illegally steals electricity (suspect, but no evidence)	427 (8.54%)
Total customers	5000

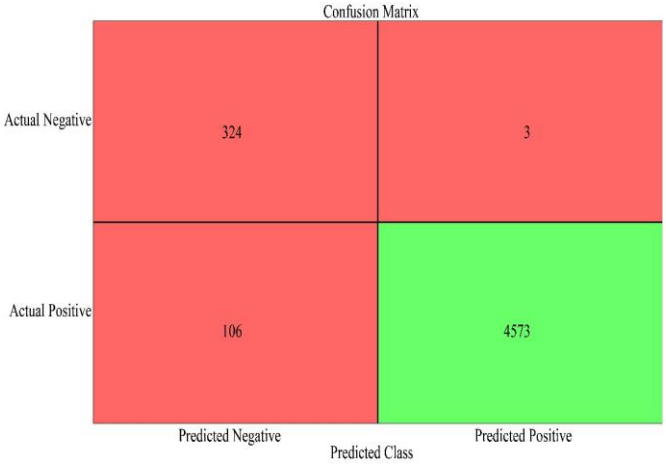

Fig. 7 Confusion matrix results

Based on the results in Figure 7, the precision, recall, F1-score, and accuracy are computed and shown in Equations (5) – (8).

$$\text{Precision} = \frac{4573}{4573+100} = 97.86\% \quad (5)$$

$$\text{Recall} = \frac{4573}{4573+3} = 99.93\% \quad (6)$$

$$\text{F1 Score} = \frac{2\times 0.9786\times 0.9993}{0.9786+0.9993} = 98.88\% \quad (7)$$

$$\text{Accuracy} = \frac{324+4573}{5000} = 97.94\% \quad (8)$$

The results in Figure 8 analyze the SVM classification outcomes; it is seen that the accuracy of the SVM to detect no theft of electricity is 0.9794 or 97.94%. The recall, on the other hand, is 99.93%. The values of precision and accuracy are almost the same and fall within the range 97%. In general, the results show that there is no stealing of electricity.

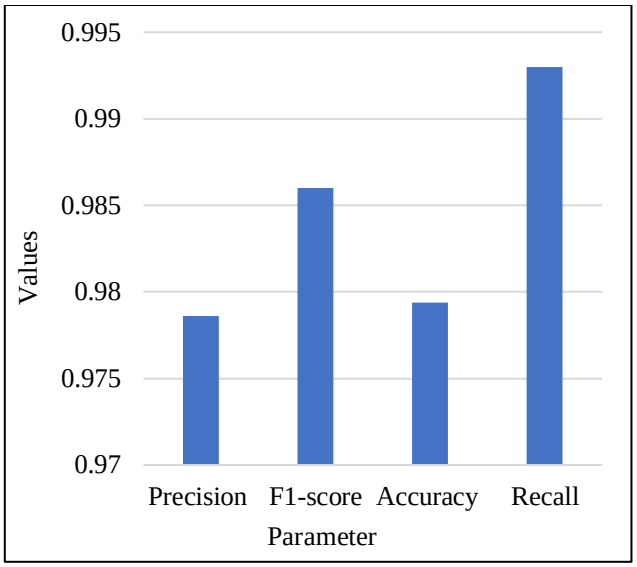

Fig. 8 Results of SVM classification

4.3. Interview Results to Support the Results of SVM

The interview findings from the 50 MVA transformer substation are shown in this section. There were 10 technicians and engineers under interview, and the themes of the interview are shown in the Thematic table in Table 1. Table 3 displays the interview findings.

Table 3. Results of interviews

Themes	Frequency
Awareness of illegal use of electricity	2
Significance of energy data	5
Overall electricity usage	3

From the interview results, it is seen that many respondents did not agree that there is an illegal use of electricity that can be viewed from the 50 MVA transformer in the substation. Many had agreed that to detect the illegal use of electricity, the system should be installed in each of the consumers' premises or built into the energy meter.

The results shown in Table 4 clearly highlight that SVM outperforms qualitative analysis across all evaluation metrics. The most significant advantage is in recall (99.3%), which means SVM ensures theft cases are rarely missed. While qualitative analysis provides around 80% consistency, it lacks the accuracy of the machine learning model. The overall results supported by the interview results can be seen in Table 4, while the comparative analysis is shown in Figure 9.

Table 4. Overall results of the research

Parameters	SVM	Qualitative analysis
Precision	0.9786	0.8 (80%)
F1-score	0.9860	0.8 (80%)
Accuracy	0.9794	0.8 (80%)
Recall	0.9930	0.8 (80%)

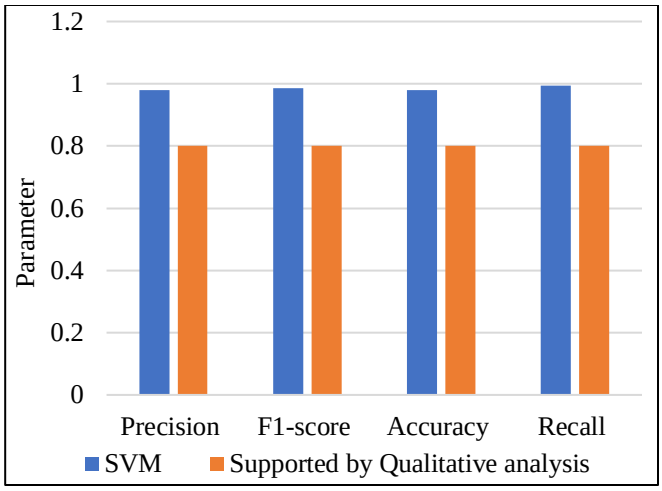

Fig. 9 Comparative analysis

Table 5. Comparison with related works

Ref.	Precision	Recall	F1-score	Accuracy
[24]	97.50%	95.00%	94.00%	93.33%
[25]	98.75%	95.45%	97.07%	97.01%
[26]	93.00%	97.00%	93.70%	95.90%
[27]	86.57%	90.78%	88.62%	88.45%
[28]	90.00%	87.00%	94.00%	89.00%
[29]	99.90%	75.70%	85.10%	94.10%
[30]	89.00%	86.00%	84.00%	86.00%
Proposed	**97.86%**	**99.93%**	**98.88%**	**97.94%**

Also, the results of this study were compared with related works of other literature, as shown in Table 5.

The results show that the proposed SVM method performed better than the compared literature works for Recall, F1-score, and Accuracy, while for Precision, it ranked second.

5. Conclusion

In this work, a comparative analysis based on SVM and qualitative techniques for energy theft detection is presented. The results showed that the SVM performed better than the qualitative analysis in detecting energy theft. Precision was 97.86%, recall was 99.93%, F1-score was 98.88%, and accuracy was 97.94%. Overall, the SVM attained more dependability, guaranteeing maximum theft detection coverage and fewer false alarms.

However, qualitative analysis showed little consistency, averaging around 80% across all parameters. Consequently, the findings verify that SVM offers a more reliable and stronger method for detecting energy theft than conventional qualitative evaluations. The future work should enlarge the dataset with more varied consumption patterns, seasonal fluctuations, and larger client bases. Also, real-time deployment with smart meters and IoT-based monitoring systems should be explored to assess practical applicability under dynamic grid conditions.

References

[1] Priyanka Ashok Bhoite, Yuvraj K. Kanse, and Supriya P. Salave, "IoT-based Electricity Theft Detection System," *International Journal of Innovative Technology and Exploring Engineering*, vol. 14, no. 7, pp. 30-35, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[2] Muhammad Sajid Iqbal et al., "A Critical Review of Technical Case Studies for Electricity Theft Detection in Smart Grids: A New Paradigm based Transformative Approach," *Energy Conversion and Management: X*, vol. 26, pp. 1-37, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[3] Potego Maboe Kgaphola, Senyeki Milton Marebane, and Robert Toyo Hans, "Electricity Theft Detection and Prevention using Technology-based Models: A Systematic Literature Review," *Electricity*, vol. 5, no. 2, pp. 334-350, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[4] Xinwu Sun et al., "Electricity Theft Detection Method based on Ensemble Learning and Prototype Learning," *Journal of Modern Power Systems and Clean Energy*, vol. 12, no. 1, pp. 213-224, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Qudus Omotayo Ajiboye et al., "Energy Theft Detection and Real-Time Monitoring in a Smart Prepaid Metering System," *Path of Science: International Electronic Scientific Journal*, vol. 10, no. 8, pp. 6029-6037, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[6] D.A. Oladosu, "Energy Theft Detector (ETD): A Salvage Module from Meter Bypassing and Illegal Tapping of Electricity," *Iconic Research and Engineering Journals*, vol. 7, no. 11, pp. 196-204, 2024. [Google Scholar] [Publisher Link]

[7] Mileta Žarković, and Goran Dobrić, "Artificial Intelligence for Energy Theft Detection in Distribution Networks," *Energies*, vol. 17, no. 7, pp. 1-17, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[8] Nwamaka Georgenia Ezeji, Kingsley Ifeanyi Chibueze, and Nnenna Harmony Nwobodo-Nzeribe, "Developing and Implementing an Artificial Intelligence (AI)-Driven System for Electricity Theft Detection," *ABUAD Journal of Engineering Research and Development (AJERD)*, vol. 7, no. 2, pp. 317-328, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[9] Xun Yuan et al., "A Novel DDPM-based Ensemble Approach for Energy Theft Detection in Smart Grids," *arXiv Preprint*, pp. 1-13, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] Rajesh K. Ahir, and Basab Chakraborty, "Pattern-based and Context-Aware Electricity Theft Detection in Smart Grid," *Sustainable Energy, Grids and Networks*, vol. 32, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Darragh Carr, and Murray Thomson, "Non-Technical Electricity Losses," *Energies*, vol. 15, no. 6, pp. 1-14, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Gheorghe Grigoras, and Bogdan-Constantin Neagu, "Smart Meter Data-based Three-Stage Algorithm to Calculate Power and Energy Losses in Low Voltage Distribution Networks," *Energies*, vol. 12, no. 15, pp. 1-27, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[13] Nadeem Javaid Pamir et al., "Electricity Theft Detection for Energy Optimization using Deep Learning Models," *Energy Science and Engineering*, vol. 11, no. 10, pp. 3575-3596, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Qingyuan Cai, Peng Li, and Ruchuan Wang, "Electricity Theft Detection based on Hybrid Random Forest and Weighted Support Vector Data Description," *International Journal of Electrical Power and Energy Systems*, vol. 153, pp. 1-15, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] Denis Hock, Martin Kappes, and Bogdan Ghita, "Using Multiple Data Sources to Detect Manipulated Electricity Meter by an Entropy-Inspired Metric," *Sustainable Energy, Grids and Networks*, vol. 21, pp. 1-14, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[16] Chun-Wei Tsai et al., "An Effective Ensemble Electricity Theft Detection Algorithm for Smart Grid," *IET Networks*, vol. 13, no. 5-6, pp. 471-485, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] Murilo A. Souza et al., "Detection of Non-Technical Losses on a Smart Distribution Grid based on Artificial Intelligence Models," *Energies*, vol. 17, no. 7, pp. 1-16, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[18] Sindhura Rose Thomas, Venugopalan Kurupath, and Usha Nair, "A Passive Islanding Detection Method based on K-Means Clustering and EMD of Reactive Power Signal," *Sustainable Energy, Grids and Networks*, vol. 23, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] Konstantinos V. Blazakis, Theodoros N. Kapetanakis, and George S. Stavrakakis, "Effective Electricity Theft Detection in Power Distribution Grids using an Adaptive Neuro Fuzzy Inference System," *Energies*, vol. 13, no. 12, pp. 1-13, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[20] Jie Lu et al., "Timing Shift-based Bi-Residual Network Model for the Detection of Electricity Stealing," *EURASIP Journal on Advances in Signal Processing*, vol. 2022, no. 1, pp. 1-14, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[21] Celimpilo Lindani Zulu, and Oliver Dzobo, "Real-Time Power Theft Monitoring and Detection System with Double Connected Data Capture System," *Electrical Engineering*, vol. 105, no. 5, pp. 3065-3083, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[22] B. Lakshman Prabhu, and E. Ashwin Kumar, "IoT based Electricity Theft Detection using Artificial Intelligence Techniques for Sustainable Electricity Usage," *International Journal of Novel Research and Development*, vol. 9, no. 1, pp. a656-a664, 2024. [Publisher Link]

[23] P. Hemalatha et al., "IoT-Driven Monitoring for Detecting and Preventing Electricity Theft in Power Networks," *International Journal of Research Publication and Reviews*, vol. 6, no. 4, pp. 10517-10527, 2025. [Publisher Link]

[24] Hasnain Iftikhar et al., "Electricity Theft Detection in Smart Grid using Machine Learning," *Frontiers Energy Research*, vol. 12, pp. 1-18, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[25] Nada M. Elshennawy, Dina M. Ibrahim, and Ahmed M. Gab Allah, "An Efficient Electricity Theft Detection based on Deep Learning," *Scientific Reports*, vol. 15, no. 1, pp. 1-15, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[26] Zahoor Ali Khan et al., "Electricity Theft Detection using Supervised Learning Techniques on Smart Meter Data," *Sustainability*, vol. 12, no. 19, pp. 1-25, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[27] Alyaman H. Massarani et al., "Efficient and Accurate Zero-Day Electricity Theft Detection from Smart Meter Sensor Data using Prototype and Ensemble Learning," *Sensors*, vol. 25, no. 13, pp. 1-21, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[28] Md. Nazmul Hasan et al., "Electricity Theft Detection in Smart Grid Systems: A CNN-LSTM based Approach," *Energies*, vol. 12, no. 17, pp. 1-18, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[29] Safdar Ali Abro et al., "Non-Technical Loss Detection in Power Distribution Networks using Machine Learning," *Scientific Reports*, vol. 15, no. 1, pp. 1-15, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[30] Nitasha Khan et al., "A Deep Learning Technique Alexnet to Detect Electricity Theft in Smart Grids," *Frontiers in Energy Research*, vol. 11, pp. 1-13, 2023. [CrossRef] [Google Scholar] [Publisher Link]