International Journal of Electrical and Computer Engineering (IJECE)
Vol. 14, No. 2, April 2024, pp. 1240~1250
ISSN: 2088-8708, DOI: 10.11591/ijece.v14i2.pp1240-1250

Machine learning-based electricity theft detection using support vector machines

Safdar Ali Abro[1], Lyu Guang Hua[2], Javed Ahmed Laghari[3], Muhammad Akram Bhayo[3], Abdul Aziz Memon[4]
[1]Department of Electrical Engineering Technology, The Benazir Bhutto Shaheed University of Technology and Skill Development Khairpur Mis, Khairpur, Pakistan
[2]Power China Huadong Engineering Corporation Limited, Hangzhou, China
[3]Department of Electrical Engineering, Quaid-e-Awam University of Engineering, Science and Technology, Nawabshah, Pakistan
[4]Department of Electrical Engineering, Sukkur IBA University, Sukkur, Pakistan

Article Info

Article history:

Received May 25, 2023
Revised Oct 23, 2023
Accepted Nov 29, 2023

Keywords:

Machine learning
Support vector machine
Electricity theft detection
sigmoid
Polynomial
Radial basis function
Linear kernel function

ABSTRACT

Electricity theft is a serious issue that many nations face, especially in developing areas where non-technical losses can make up a significant percentage of the overall losses sustained by utilities. Electricity theft detection (ETD) is a very challenging task because it frequently introduces irregularities in customer electricity consumption patterns. In recent times, machine learning (ML) techniques have been investigated as a potential solution for ETD. In this research, author propose electricity theft detection based on four kernel functions of support vector machines (SVM). The proposed method analyzes the electricity consumption patterns and then predicts the category of the user. The kernel functions utilized includes polynomial, sigmoid, radial basis function (RBF) and linear kernel function. For experimentation and model training, a dataset of Pakistani utility company is used, which contains the electricity consumption information. The results highlight SVM method works well for accurate ETD. The detection accuracy of the various kernel functions of SVM is 83%, 79%, 80%, and 76% for RBF, polynomial, sigmoid, and linear kernel functions, respectively, demonstrating the effectiveness of the proposed SVM-based method for theft detection. By leveraging these ML-based methods, utility companies can strengthen their ability to detect and prevent electricity theft, leading to improved revenue management and dependability of services.

Corresponding Author:

Safdar Ali Abro
Department of Electrical Engineering Technology, Faculty of Engineering and Technology, The Benazir Bhutto Shaheed University of Technology and Skill Development Khairpur Mis
66020, Sindh, Pakistan
Email: safdar@bbsutsd.edu.pk

1. INTRODUCTION

Electricity theft is indeed a serious issue in many countries, and it has significant economic, social, and environmental implications. Traditional methods for detecting electricity theft often rely on manual inspections and periodic meter readings, which can be inefficient and may not effectively identify all instances of theft [1]. The World Bank estimates that theft of power costs the global economy $96 billion every year in lost income [2]. Electricity theft is especially common in developing countries, where non-technical losses can make up a significant share of all utility losses [3]. Physical examination and manual meter reading are two outdated, expensive, time consuming and error-prone methods of detecting electricity theft [4]. As a result, there has been a growing interest in developing more advanced and technology-driven

approaches to address this problem. In recent times, machine learning (ML) techniques have been investigated as a potential solution for automatically detecting the electricity theft and it has shown the promising results. Machine learning algorithms can analyze large data sets, which can also identify patterns that might be signs of electricity theft [5], [6]. One of the commonly used machine learning algorithm i.e., support vector machines (SVM) has been effectively used in a number of industries, including banking, healthcare, and cyber security and Electric theft detection [7]. As a supervised learning system, SVM, can identify distinct data classes and generate predictions based on discovered patterns [8], [9].

In this article, author suggest using SVM and its four-kernel function to automatic detection and prediction of electricity theft by analyzing the consumption patterns of the users. Support vector machines (SVMs) are a type of supervised machine learning algorithm. SVMs work by finding a hyperplane that best separates data points belonging to different classes while maximizing the margin between the two classes. Here's how SVMs can be applied to detect electric theft:

- Data collection: to detect electrical theft, you need a dataset with details on typical patterns of electricity use and pertinent attributes. This dataset should be tagged, indicating that it includes illustrations of both typical electricity use (which is not theft) and cases of theft.
- Feature extraction: extract useful characteristics from your dataset using the feature extraction method. These characteristics can include trends in electricity consumption over time, variations in voltage and power factor, and any other pertinent data that might aid distinguish between legitimate use and theft.
- Data preprocessing: preprocessing your data includes cleaning and preparing it. The handling of missing values, normalization of the data, and division of the data into training and testing sets could all be included in this stage.
- Training the SVM: now, you can train your SVM model using the labeled training data. The SVM algorithm's objective is to find a hyperplane that best separates the two classes (normal and theft) while maximizing the margin. This hyperplane is chosen to ensure that it is as far away from the nearest data points of both classes as possible. Mathematically, the SVM optimization problem can be represented as in (1):

$$Min\ f: ½\ ||w||2$$
$$s.t.\ g: yi\ (w \bullet xi\ ) - b = 1\ or\ [yi\ (w \bullet xi\ ) - b] - 1 = 0 \quad (1)$$

  where w is the weight vector, xi represents the feature vector of the i^{-th} training example, b is the bias term, and yi is the class label for the i^{-th} training example (-1 for normal, +1 for theft).
- Kernel trick: SVMs can translate data into a higher-dimensional space where separation is achievable using a kernel function in situations where the data is not linearly separable. The polynomial kernel and the radial basis function (RBF) kernel are examples of common kernel functions. The type of data determines which kernel function to use.
- Decision making: once the SVM model is trained, you can use it to classify new data points. For electric theft detection, if a new data point is classified as +1 (theft), it suggests that the consumption pattern is likely indicative of theft, while a classification of -1 (normal) indicates normal electricity consumption.
- Evaluation: evaluate the performance of your SVM model using metrics such as accuracy, precision, recall, and F1-score on a separate testing dataset. This helps you assess how well your model is performing in detecting electric theft.
- Fine-tuning: you can further fine-tune your SVM model by adjusting hyperparameters, such as the regularization parameter (C) or the kernel parameters, to optimize its performance.

In summary, SVM can be a valuable tool for electric theft detection by learning patterns from historical data and classifying new consumption patterns as normal or indicative of theft [10]. The suggested approach entails gathering information on electricity usage and training an SVM model to distinguish between regular and irregular consumption patterns. The classification of electricity usage data and the detection of electricity theft are subsequently performed using the SVM mode [11], [12]. Our research focuses on assessing the performance of the suggested SVM-based strategy in identifying electricity theft and contrasting it with different kernel functions.

Electricity theft is a significant problem affecting utilities worldwide, and various methods have been proposed to detect and prevent it [13]. Traditional methods of detecting electricity theft, such as physical inspection and manual meter reading, are time-consuming, expensive, and error-prone [14]. As such, there is growing interest in using machine learning techniques to detect electricity theft. To identify electricity theft, several research employ machine learning methods such as artificial neural networks (ANNs), decision trees (DTs), SVMs, and random forests (RFs). For example, a study by [15] proposed model uses features extracted from monthly consumption data to segregate normal electricity consumption (non-theft)and theft customers, selecting the most relevant features using the Pearson's chi-square feature

selection algorithm, and classifying them using the Boosted C5.0 Decision Tree algorithm. This method can assist distribution system operators (DSOs) in their fight against electricity theft.

Another study by Ghaedi *et al.* [16] proposed a method for electricity theft detection based on a combination of an improved crow search algorithm and support vector machines. The proposed method analyzed customer electricity consumption data provided by meters and combined the algorithms to classify electricity consumption patterns as normal or theft. This study reported pretty good accuracy in classifying the consumers. SVMs are also commonly used to detect electricity theft. A study by Nagi *et al.* [17] used SVMs to detect electricity theft by analyzing customer load profiles. The proposed method extracted features from load profiles and used SVM to classify electricity consumption patterns as normal or theft. The study confirmed reasonable accuracy in detecting electricity theft using SVM. Another study by *et al.* [18] proposed a novel convolutional neural network based (CNN) method with RUSBoost manta-ray foraging optimization and RUSBoost bird swarm algorithm for detecting electricity theft by analyzing customers' electricity consumption patterns. The proposed method included data preprocessing, feature extraction, model training, and standard or abnormal classification of electricity expenditure patterns.

In summary, machine learning techniques have emerged as a promising solution to the problem of electricity theft detection. Several studies have proposed using machine learning algorithms such as ANN, decision trees, SVM, and random forest to detect electricity theft. Among these algorithms, proposed technique shows promising results in detecting electricity theft in this study, by analyzing customers' electricity consumption patterns [19], [20].

2. METHOD

The technique used in the workflow to identify electricity theft essentially consists of five steps, as indicated in Figure 1. It starts with collection of data, preprocessing data, feature extraction, model training and finally testing of model. The workflow's components will be described in depth in accordance with Figure 1.

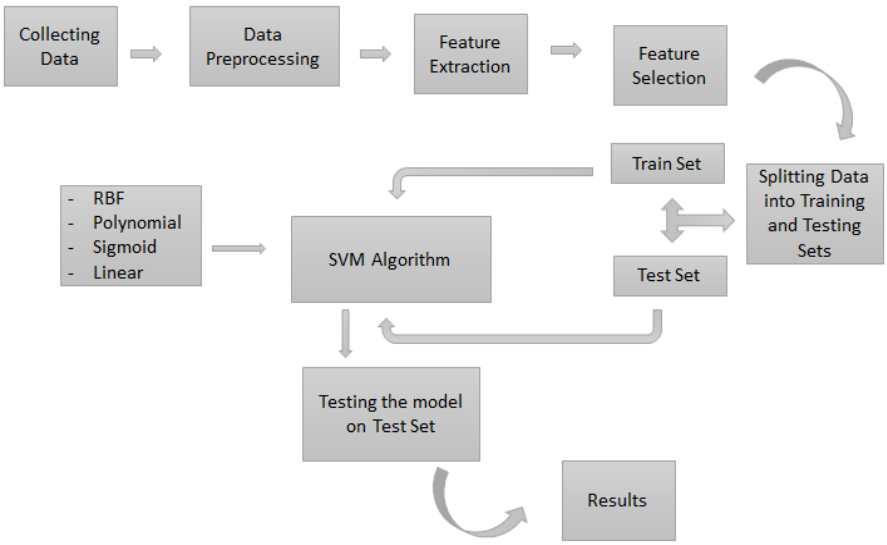

Figure 1. A flowchart for the suggested electricity theft detection (ETD) model

2.1. Data collection

The first step is to collect electricity consumption data from customers. This data can be collected from smart meters and other electronic devices that record electricity consumption on a regular basis. For this research, Author received data from a Pakistan utility company (MEPCo) that included monthly electricity consumption data for a large no. of customers over a three-year period. The temporality range of the data, which comprises from May, 2015 to April, 2018 (approximately 36 Months). The file size is 17.3 MB in CSV format, with respect to the data structure of the Data set is comprised of normal electricity consumption (non-theft) customers amounting 2,117 (77%) and theft customers amounting 646 (23%) as describe in Table 1.

Table 1. Customers divided into no. of groups

Total No. of customers	Normal electricity consumption (non-theft)	Theft customers	Test set	Training set
2,763	2,117	646	1,934	829

2.2. Data preprocessing

This step is very important to convert raw data into useful data set so model can easily learn from useful data to generate predictions. Collected data may contain errors, missing values, or outliers that need to be addressed before training an SVM model. Preprocess the data to remove missing values and outliers, normalize the data, and have all features on the same scale. The interpolation approach, which is illustrated by the (2), is used to recover missing values from the dataset of the relevant research.

$$F(x) = \begin{cases} \frac{(x_{i+1}+x_{i-1})}{2} & if\ x_i \in NaN, x_{i-1}\ and\ x_{i+1} \notin NaN \\ 0 & if\ x_i \in NaN, x_{i-1}\ or\ x_{i+1} \in NaN \\ x_i & if\ x_i \notin \end{cases} \quad (2)$$

where, x_i represents electricity consumption data and NaN represents non-numeric value.

Additionally, it is discovered that the statistics on power use contain incorrect figures (or outliers). Specifically, apply the "three-sigma rule of thumb" to recover the value using (3).

$$f(x_i) = \begin{cases} avg(x) + 2.std(x), & if\ x_i > avg(x) + 2.std(x) \\ x_i & otherwise \end{cases} \quad (3)$$

where $avg(x)$ represents the average value of x and $std(x)$ represents the standard deviation of x, and x is a vector made up of x_i per day. In (3), only take positive deviation because each user's electricity use is always higher than 0. In conclusion, the outliers may be successfully mitigated using this strategy.

2.3. Feature extraction

Extracts features from the preprocessed data can be used to train an SVM model. In machine learning and signal processing, the process of extracting pertinent information or features from unprocessed data is known as feature extraction [21]. It involves transforming the input data into more compact and representative feature representation that captures the important characteristics of the data. The extracted features include average hourly electricity usage, hourly electricity usage variance, and total daily electricity usage, mean, standard deviation, peak to peak, skewness, and kurtosis. Some of important features are defined further as follows.

2.3.1. Skewness

The asymmetry of the dataset or probability distribution is measured by skewness. When the skewness of the data is positive, it means that the data is skewed to the right (tail on the right side), and when it is negative, it means that the data is skewed to the left. A symmetric distribution is indicated in (4) with a skewness value of 0.

$$Skewness = \frac{\sum_{i=1}^{N}(Xi-\dot{X})3}{N.\sigma 3} \quad (4)$$

where in the dataset, x_i stands for every single data point; $\dot{X}$ represents the dataset mean or average; N is the number of data points; and σ is the standad deviation of the dataset.

2.3.2. Kurtosis

Kurtosis quantifies the way flat or peaky a dataset or probability distribution is in comparison to a normal distribution. It indicates if the data is more leptokurtic (heavy tails) or platykurtic (light tails) than a normal distribution. The kurtosis of a normal distribution is commonly represented by a value of 3, which is frequently used as a benchmark. Data with a heavy tail (leptokurtic) value is greater than three, whereas data with a light tail (platykurtic) value is less than three. The formula for kurtosis, known as excess kurtosis, is typically calculated as in (5).

$$Kurtosis\ = \frac{\sum_{i=1}^{N}(Xi-\dot{X})4}{N.\sigma 4} - 3 \quad (5)$$

where x_i stand for each individual data point in the dataset, $\dot{X}$ is the mean (average) of dataset, N is the number of data points, and σ is the standad deviation of the dataset.

2.4. Training SVM model

The extracted features from preprocessed data are used to train the SVM model. The SVM model is a supervised machine learning algorithm that learns to distinguish between normal and theft electricity consumption patterns. Although it can also be used to handle multi-class classification, it works especially well at solving binary classification problems [22]. SVM's fundamental goal is to partition data points into distinct classes in a high-dimensional feature space by identifying the best hyperplane. The hyperplane is selected so as to optimize the margin, or the separation between the hyperplane and the closest data points for each class. It identify the data points that are closest to the hyperplane as support vectors.

Kernel functions are an essential component of several machine learning algorithms, including SVM [23]. These functions can transform input data into a higher-dimensional space, enabling the algorithms to identify complex hidden relationships in the data and make accurate predictions. In this study four kernel functions i.e., RBF, polynomial, sigmoid, and linear kernel functions in the context of SVM are used.

2.5. Test SVM model

After the SVM model is trained, test it on the rest of the data to evaluate its performance. Measure model accuracy and false positive rate. Based on learned patterns, the SVM model categorizes electricity consumption data as normal or abnormal. Abnormal electricity usage patterns indicate electricity theft and are flagged for further investigation. Finally, evaluate the performance of the proposed method in terms of accuracy, false positive rate, and computational complexity. Comparing the performance of each SVM kernel function used in the paper.

3. RESULTS AND DISCUSSION

Electricity theft detection in supervised learning is primarily concerned with the issue of class imbalance. The proportion of normal electricity consumption (non-theft) consumers in this situation is really different from the amount of these theft ones. Consequently, a straightforward accuracy metric is unreliable for assessment. Different performance measures are taken into account in this research. The values of these assessment measures are derived from the confusion matrix.

3.1. Confusion matrix

A table known as a confusion matrix is used to assess how well a classification algorithm performs. It shows the proportion of true positives, true negatives, false positives, and false negatives in a given set of forecasts. True positive (TP), the theft customers correctly identified as being theft. False positive (FP), the normal customers incorrect identified as thieves. True negative (TN), the normal customers correctly identified as being normal. False negative (FN), the theft customers identified as being normal.

There are other validation parameters such as accuracy, Matthew's correlation coefficient (MCC), area under curve (AUC), area under receiver operating characteristic curve (ROC AUC), area under the precision recall curve (PR AUC), precision, recall and F1 score are used in this study.

- Accuracy is defined as the percentage of correctly predicted data points among all the data points which is given in (6). It is a commonly used statistic in the data science profession for categorization issues. Where the distribution of labels is unbalanced, it is not regarded as a valid measure.

$$accuracy = \frac{TP+TN}{TP+TN+FP} \times 100\% \quad (6)$$

- MCC: the true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN) all four components of the confusion matrix are taken into consideration by the Matthews correlation coefficient. MCC score ranges between -1 to 1, A value of 1 indicates an accurate prediction, a value of 0 indicates no class separation capability, and a value of -1 indicates an incorrect prediction. It is formulated in [24] using (7).

$$MCC = \frac{TP \times TN - FP \times FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}} \quad (7)$$

- AUC: as given in (8), the area under the ROC curve is a performance parameter that is used to determine how well a classification model performs overall. Plotting the true positive rate (TPR) against the false positive rate (FPR) at various threshold settings yields the ROC curve. AUC has a range of 0 to 1, with 1

denoting the best possible classifier, 0.5 denoting a random classifier, and 0 denoting the worst possible classifier.

$$AUC = \frac{\sum Rank_{i \in positiveclass} - \frac{M(1+M)}{2}}{M \times N} \quad (8)$$

- ROC-AUC: it displays a graphical depiction of a model to assess how well it detects. The capacity of the classifier to distinguish between two classes is improved when the ROC-AUC is near to 1. The TPR and FPR of the model's trade-off are solely summarized by ROC-AUC.
- PR-AUC: this performance metric calculates the area under the precision-recall curve to assess a classification model's general performance. The precision-recall curve is produced by plotting precision (positive predictive value) vs recall (true positive rate) at various threshold values. On a scale of 0 to 1, 1 represents the ideal classifier, 0.5 represents a random classifier, and 0 represents the impossibly inaccurate classifier [25].
- Precision: in (9), the percentage of true positives (TP) out of all positive predictions (TP + FP) is known as precision. In other words, it assesses the precision of the model's successful predictions. A high precision indicates that the model has a low rate of false positives and is effective at predicting real positives [26].

$$Precision = \frac{TP}{TP+FP} \quad (9)$$

- Recall: recall is the percentage of genuine positive cases that are true positives (TP) as opposed to false negatives (FN). In other words, it assesses how well the model can recognize positive situations. A high recall indicates that the model finds the majority of positive cases and detects few false negatives. Using (10) mentioned in (10).

$$Recall(DR) = \frac{TP}{TP+FN} \quad (10)$$

- F1 score: It is the precision and recall weighted harmonic mean. The F1 score is helpful in circumstances when FP and FN are equally significant because it strikes a compromise between accuracy and memory. A high F1 score indicates that the model has a high recall and accuracy, which is given in (11).

$$F1 = 2 \times \frac{Precision \times Recall}{Precesion + Recall} \quad (11)$$

The outcomes for each comparison techniques are shown in this section. The dataset was divided into two sets, the training set and the testing set. Confusion matrix of the four kernel functions used in this research on a given dataset is shown in Figure 2. Confusion matrix of RBF kernel function shown in Figure 3.

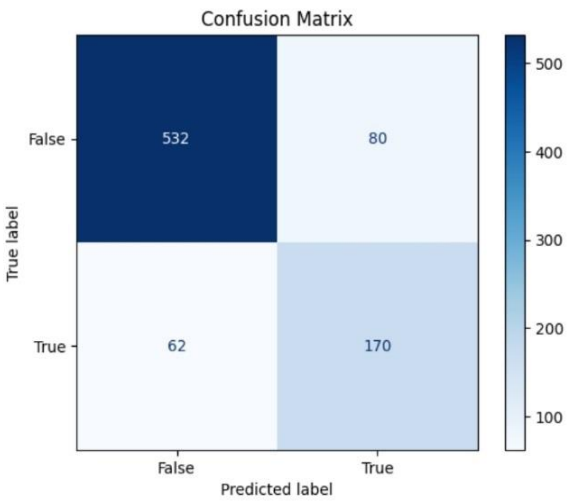

Figure 2. Confusion matrix of RBF kernel function

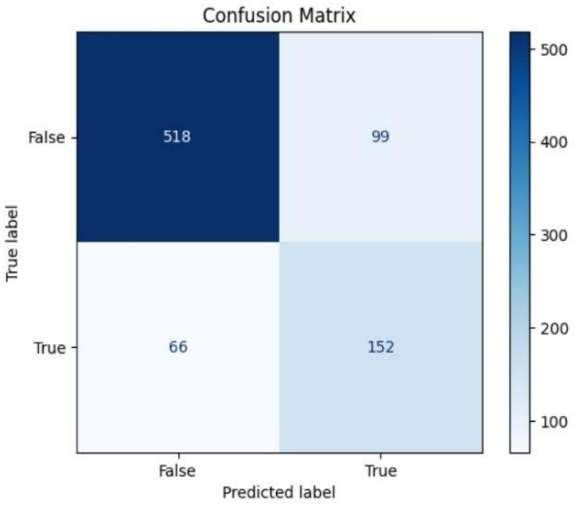

Figure 3. Confusion matrix of polynomial function

Confusion matrix of polynomial function shown in Figure 4. Confusion matrix of sigmoid kernel function, and Figure 5 confusion matrix of linear kernel function. In Table 2 shows the comparative analysis of the performance of the four kernel functions is presented.

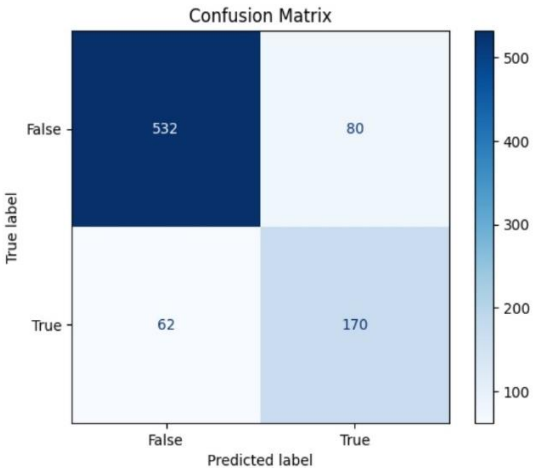

Figure 4. Confusion matrix of sigmoid kernel function

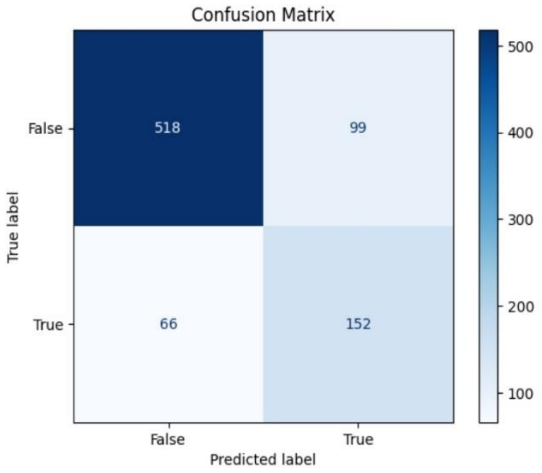

Figure 5. Confusion matrix of linear kernel function

Table 2. Validation table of the four kernel functions

Kernel function	Accuracy	MCC	AUC	ROC AUC	PR AUC
RBF	83%	0.39	0.88	0.88	0.73
Sigmoid	79%	0.16	0.53	0.53	0.33
Polynomial	80%	0.20	0.86	0.86	0.64
Linear	76%	0.12	0.77	0.77	0.42

3.2. RBF kernel

The RBF kernel has the highest accuracy, ROC AUC, and PR AUC among the kernels in the table. This suggests that it performs the best overall on the given dataset. The MCC value indicates moderate agreement between predictions and actual outcomes.

3.3. Sigmoid kernel

The Sigmoid kernel exhibits an accuracy of 79%, with an MCC of 0.16, indicating lower agreement compared to other kernels. The AUC and ROC AUC values are 0.53, reflecting mediocre discrimination ability. The PR AUC of 0.33 suggests a suboptimal precision-recall trade-off, indicating that the sigmoid kernel may not be well-suited for this particular dataset.

3.4. Polynomial kernel

The polynomial kernel achieves an accuracy of 80%, with an MCC of 0.20, indicating improved agreement compared to the sigmoid kernel. The AUC and ROC AUC values of 0.86 suggest good discrimination ability, and the PR AUC of 0.64 indicates a favorable precision-recall trade-off. Overall, the Polynomial kernel demonstrates a balanced performance on multiple evaluation metrics.

3.5. Linear kernel

The linear kernel has the lowest accuracy among the presented kernels at 76%, with an MCC of 0.12, indicating relatively low agreement. The AUC and ROC AUC values of 0.77 suggest acceptable discrimination ability. However, the PR AUC of 0.42 indicates a suboptimal precision-recall trade-off, highlighting potential limitations in capturing positive instances effectively.

The RBF kernel appears to be the best-performing kernel for this dataset, as it has the highest accuracy as shown in Figure 6 and the best ROC AUC and PR AUC values. The polynomial kernel also performs well, while the sigmoid kernel performs poorly in comparison. The choice of kernel function should consider the specific goals of the machine learning task, and further analysis, including hyperparameter tuning, may be needed to optimize the model's performance. In Table 3 determined the performance of the mentioned kernel functions using three other validation parameters.

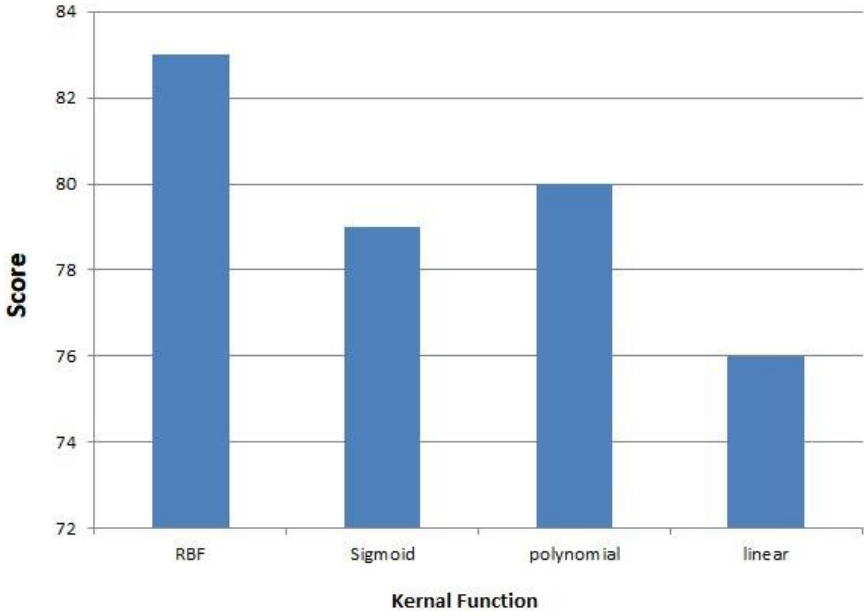

Figure 6. Comparison graph of SVM kernel functions

Table 3. Precision, recall, and F1 score of all four kernel functions

Kernel function	Precision	Recall	F1 score
RBF	0.84	0.83	0.78
Sigmoid	0.75	0.79	0.72
Polynomial	0.79	0.80	0.73
Linear	0.72	0.78	0.70

3.6. RBF kernel

The RBF kernel achieves a high precision, recall, and F1 score. This suggests that it has a good balance between making accurate positive predictions (precision) and capturing most of the positive instances in the dataset (recall). The F1 score, which combines both precision and recall, also indicates good overall performance.

3.7. Sigmoid kernel

The Sigmoid kernel has a slightly lower precision compared to the RBF kernel indicating a higher rate of false positives. However, its recall is still relatively high, capturing a substantial portion of the actual positive instances. The F1 score, while lower than the RBF kernel, indicates decent overall performance.

3.8. Polynomial kernel

The polynomial kernel shows good precision and recall values. The F1 score is moderate at 0.73, reflecting a balance between precision and recall. It performs well in terms of both precision and recall and achieves a respectable F1 score.

3.9. Linear kernel

The linear kernel has the lowest precision among the kernels, but it compensates with a relatively high recall. However, the F1 score, which combines both precision and recall, is lower compared to the other kernels, indicating that it may not perform as well in achieving a balance between precision and recall. The choice of kernel function should be based on the specific goals and requirements of the machine learning task. If precision is of utmost importance, the RBF kernel appears to be the best choice. If a balance between precision and recall is desired, both the RBF and polynomial kernels perform well. The sigmoid kernel also performs reasonably well. The linear kernel may be suitable if higher recall is more important than precision, but it has a lower F1 score compared to the other kernels. Further analysis and consideration of the application context are necessary to make an informed decision about which kernel to use. Figure 7 illustrates the comparison of mentioned kernel functions.

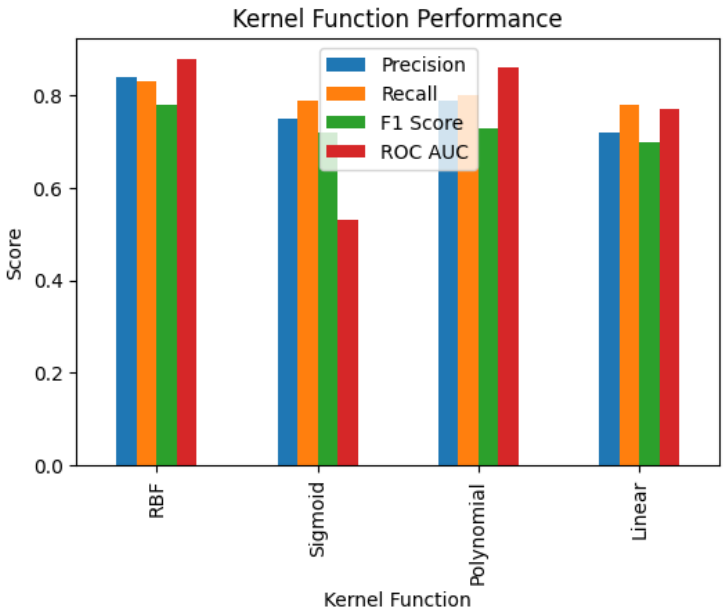

Figure 7. Comparison of SVM kernel functions

4. CONCLUSION

This research has analyzed the performance results of the support vector machine technique with four kernel functions for electricity theft detection. Performance was evaluated using accuracy, precision, recall, F1-score, and AUC for all functions. Compared to the results of this study, it can be concluded that SVM with the RBF kernel is the most effective kernel function for electricity theft detection. The RBF kernel function achieved the highest accuracy rate compared to other kernel functions that were tested in the study. The use of SVM with RBF kernel function is a promising approach for electricity theft detection in the power sector. Overall, the results of this study demonstrate the potential of SVM with RBF kernel function as a reliable and accurate tool for electricity theft detection in the power sector.

REFERENCES

[1] T. B. Smith, "Electricity theft: a comparative analysis," *Energy Policy*, vol. 32, no. 18, pp. 2067–2076, Dec. 2004, doi: 10.1016/S0301-4215(03)00182-4.
[2] A. Foster, V and N. Pushak, "Ghana's infrastructure: a continental perspective," *The Oxford Handbook of Religious Diversity*, 2010.
[3] D. Carr and M. Thomson, "Non-technical electricity losses," *Energies*, vol. 15, no. 6, Mar. 2022, doi: 10.3390/en15062218.
[4] M. Lisowski, R. Masnicki, and J. Mindykowski, "PLC-enabled low voltage distribution network topology monitoring," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6436–6448, Nov. 2019, doi: 10.1109/TSG.2019.2904681.
[5] M. Nazmul Hasan, R. N. Toma, A. Al Nahid, M. M. Manjurul Islam, and J. M. Kim, "Electricity theft detection in smart grid systems: A CNN-LSTM based approach," *Energies*, vol. 12, no. 17, Aug. 2019, doi: 10.3390/en12173310.
[6] K. Fatima, M. Rafique, A. M. Soomro, and M. Kumar, "Tailoring hydrogen adsorption and desorption properties of Li-doped SV (single vacancy) monolayer h -BN systems using ab initio calculations," *Canadian Journal of Physics*, vol. 101, no. 11, pp. 673–685, Nov. 2023, doi: 10.1139/cjp-2023-0072.
[7] I. H. Sarker, "Machine learning: algorithms, real-world applications and research directions," *SN Computer Science*, vol. 2, no. 3, May 2021, doi: 10.1007/s42979-021-00592-x.
[8] H. Kaur and V. Kumari, "Predictive modelling and analytics for diabetes using a machine learning approach," *Applied Computing and Informatics*, vol. 18, no. 1–2, pp. 90–100, Jul. 2022, doi: 10.1016/j.aci.2018.12.004.
[9] A. Hussain, G. Ali, F. Akhtar, Z. H. Khand, and A. Ali, "Design and analysis of news category predictor," *Engineering, Technology and Applied Science Research*, vol. 10, no. 5, pp. 6380–6385, Oct. 2020, doi: 10.48084/etasr.3825.
[10] M. Ali *et al.*, "Low profile wind savonius turbine triboelectric nanogenerator for powering small electronics," *Sensors and Actuators A: Physical*, vol. 363, Dec. 2023, doi: 10.1016/j.sna.2023.114535.
[11] P. P. Biswas *et al.*, "Electricity theft pinpointing through correlation analysis of master and individual meter readings," *IEEE Transactions on Smart Grid*, vol. 11, no. 4, pp. 3031–3042, Jul. 2020, doi: 10.1109/TSG.2019.2961136.
[12] L.-G. Hua *et al.*, "Comparative analysis of power output, fill factor, and efficiency at fixed and variable tilt angles for polycrystalline and monocrystalline photovoltaic panels—the case of sukkur IBA University," *Energies*, vol. 15, no. 11, May 2022, doi: 10.3390/en15113917.
[13] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Electricity theft: overview, issues, prevention and a smart meter based approach to control theft," *Energy Policy*, vol. 39, no. 2, pp. 1007–1015, Feb. 2011, doi: 10.1016/j.enpol.2010.11.037.
[14] F. Zhou *et al.*, "A comprehensive survey for deep-learning-based abnormality detection in smart grids with multimodal image data," *Applied Sciences (Switzerland)*, vol. 12, no. 11, May 2022, doi: 10.3390/app12115336.

[15] M. S. Saeed *et al.*, "An efficient boosted C5.0 decision-tree-based classification approach for detecting non-technical losses in power utilities," *Energies*, vol. 13, no. 12, Jun. 2020, doi: 10.3390/en13123242.
[16] H. Ghaedi, S. R. Kamel Tabbakh, and R. Ghaemi, "Improving electricity theft detection using combination of improved crow search algorithm and support vector machine," *Majlesi Journal of Electrical Engineering*, vol. 15, no. 4, pp. 63–75, Dec. 2021, doi: 10.52547/mjee.15.4.63.
[17] J. Nagi, A. M. Mohammad, K. S. Yap, S. K. Tiong, and S. K. Ahmed, "Non-technical loss analysis for detection of electricity theft using support vector machines," in *2008 IEEE 2nd International Power and Energy Conference*, Dec. 2008, pp. 907–912, doi: 10.1109/PECON.2008.4762604.
[18] R. Akram *et al.*, "Towards big data electricity theft detection based on improved RUSBoost classifiers in smart grid," *Energies*, vol. 14, no. 23, Dec. 2021, doi: 10.3390/en14238029.
[19] W. Zhu, N. Zeng, and N. Wang, "Sensitivity, specificity, accuracy, associated confidence interval and ROC analysis with practical SAS® implementations.," *Northeast SAS Users Group 2010: Health Care and Life Sciences*, pp. 1–9, 2010.
[20] Z. Zheng, Y. Yang, X. Niu, H. N. Dai, and Y. Zhou, "Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1606–1615, Apr. 2018, doi: 10.1109/TII.2017.2785963.
[21] S. H. Hussain, A. Hussain, R. Shah, and S. A. Abro, "Mini rover-object detecting ground vehicle (UGV)," *University of Sindh Journal of Information and Communication Technology*, vol. 3, no. 2, pp. 104–108, 2019.
[22] L. K. Ramasamy, S. Kadry, Y. Nam, and M. N. Meqdad, "Performance analysis of sentiments in Twitter dataset using SVM models," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 3, pp. 2275–2284, Jun. 2021, doi: 10.11591/ijece.v11i3.pp2275-2284.
[23] M. Zulqarnain, R. Ghazali, Y. M. M. Hassim, and M. Rehan, "Text classification based on gated recurrent unit combines with support vector machine," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 4, pp. 3734–3742, Aug. 2020, doi: 10.11591/ijece.v10i4.pp3734-3742.
[24] I. Slimani *et al.*, "Automated machine learning: the new data science challenge," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 4, pp. 4243–4252, Aug. 2022, doi: 10.11591/ijece.v12i4.pp4243-4252.
[25] A. Botchkarev, "Performance metrics (error measures) in machine learning regression, forecasting and prognostics: Properties and typology," 2018, *arXiv:1809.03006*.
[26] D. V. Carvalho, E. M. Pereira, and J. S. Cardoso, "Machine learning interpretability: A survey on methods and metrics," *Electronics*, vol. 8, no. 8, Jul. 2019, doi: 10.3390/electronics8080832.

BIOGRAPHIES OF AUTHORS

Safdar Ali Abro holds bachelor's and master's degree in electrical engineering. Currently working as an assistant professor at the Department of Electrical Engineering Technology, The Benazir Bhutto Shaheed University of Technology and Skill Development Khairpur Mirs. His research interests include power quality, power generation, power supply quality and artificial intelligence. He can be contacted at email: safdar@bbsutsd.edu.pk.

Lyu Guang Hua received the B.S. in electric engineering from the Rocket Force Engineering University, China, in 2009. From 2010-2014, he was an engineer with Xin Jiang Goldwind Science and Technology co, Ltd. From 2014-now, he was an EPC project manager with Power China Huadong Engineering Corporation Limited. His research interest includes the wind power generation and wind project construction and O&M. He can be contacted at email: Lv_gh@hdec.com.

Javed Ahmed Laghari holds BE electrical from BUET Khuzdar, Pakistan, in 2007 and his ME and Ph.D. in electrical power from the University of Malaya, in 2012 and 2015 respectively. Currently, He is working as an associate professor in the Electrical Engineering Department, QUEST Nawabshah. His main research interest includes power system control in smart grid, islanding operation in distributed generation, conventional, adaptive, and intelligent load shedding schemes, islanding detection techniques, load frequency control of mini hydro power plants. He has published more than 30 technical papers in journals and IEEE conferences at the international level. He can be contacted at email: javed@quest.edu.pk.

Muhammad Akram Bhayo holds B.E. electrical from QUEST, Nawabshah, Pakistan in 2004 and the M.Sc. (electrical and electronic engineering from University of Duisburg-Essen, Germany, in 2013 and Ph.D. (electrical engineering) from Universiti Teknologi Malaysia, in 2021. Currently working as an assistant professor in Department of Electrical Engineering, QUEST. His current research interests include, electrical drives, modeling and simulation of wind electricity conversion system, with focus on implementation of adaptive neuro fuzzy inference system-based controllers in wind turbine emulator. He can be contacted at email: bhayoakram@quest.edu.pk.

Abdul Aziz Memon has more than fifteen years of experience in academia and industry. He is affiliated with Sukkur IBA University since January 2012, and there he is working as an associate professor at the Department of Electrical Engineering, Sukkur IBA University Pakistan. He completed his M.S. and Ph.D. level education at the Department of Electronic and Computer Engineering, Hanyang University, South Korea in year 2010 and 2018 respectively. He can be contacted at email: aziz.memon@iba-suk.edu.pk.