Development of an Integrated AI Model Based on CNN-SVM for Electricity Theft Detection

NENCHIN EMMANUEL, ADEMOH A. ISAH
Department of Electrical and Electronics Engineering,
Federal University of Technology Minna,
Minna, Niger State,
NIGERIA

Abstract: - This research presents the development and implementation of an integrated artificial intelligence model for electricity theft detection, combining Convolutional Neural Networks (CNN) and Support Vector Machines (SVM). The primary objective was to create a more accurate, efficient, and scalable method for identifying fraudulent electricity consumption patterns. Our CNN-SVM hybrid model leverages CNNs for automatic feature extraction from complex consumption data and SVMs for effective classification. This synergy allows for superior performance in detecting subtle anomalies indicative of electricity theft. The methodology involved pre-processing a large dataset of electricity consumption records, training the CNN to extract relevant features, and optimising the SVM classifier to distinguish between normal and fraudulent patterns. We evaluated the model's performance using metrics including accuracy, precision, recall, F1-score, and ROC AUC. Results demonstrated that our integrated CNN-SVM model significantly outperformed conventional machine learning techniques and standalone models in electricity theft detection. The model achieved an accuracy of 96.6%, with a precision of 97.2% and a recall of 96.1%. Comparative analysis against other state-of-the-art algorithms revealed consistently superior performance across all evaluation metrics. To enhance practical applicability, we developed and deployed a web application that implements the model, allowing for user-friendly interaction and real-time theft detection. This addition bridges the gap between research and real-world implementation, providing utility companies with an accessible tool for fraud detection. The study also explored the model's potential for real-time application and scalability to large-scale utility operations. Our findings suggest that the computational efficiency of the CNN-SVM model, coupled with the web application, offers utility companies a powerful and accessible tool for rapid response to potential fraud. This research contributes to the field of electricity theft detection by introducing a novel, high-performance AI model with a practical web-based implementation. The proposed approach not only improves detection accuracy but also offers potential for immediate real-world application, paving the way for more effective fraud prevention in the utility sector.

Key-Words: - Electricity Theft Detection, Artificial Intelligence, Machine Learning, Deep Learning, CNN, SVM

Received: April 16, 2024. Revised: September 28, 2024. Accepted: November 9, 2024. Published: December 10, 2024.

1 Introduction

Electrical energy theft or non-technical loss (NTL) is the unlawful usage of energy from the grid and is performed without accurate metering and payment, [1]. This poses a major problem for electricity distribution companies who have significant losses and unstable networks, with losses deprioritising investments in upgrading the grid infrastructure, [2], [3]. According to Onat in 2008, 14.4% of Turkey's electricity was used illegally, costing approximately $895.3 million, [4]. The value of electricity stolen annually in relatively poorer developing countries accounts for billions of dollars in losses annually, [5], as said by Messinis and Hatziargyriou.

Electrical energy theft has a significant effect on Nigeria's power sector sustainability as described by Tsado and Abel in 2022, and acts as a bottleneck to nation building strides in Nigeria, [6]. Now, this rampant theft not only robs genuine consumers of quality power supply but also disincentivizes capital inflows to upgrade and expand the grid, ensuring this cycle to go on indefinitely, [7].

Manual metre reading and physical inspections are the primary ways in which electricity theft is traditionally detected. These approaches are slow, manpower eating and not always successful in finding high-level theft methods implemented by thieves. Moreover, some new methods presented for bypass detection problems are metre tampering,

unauthorised load manipulation and bypass connections, [8], [9]. However, that abridgment is too good to be true and manual inspections may miss important regions throughout a distribution network detecting the majority of cases of theft.

The development of smart grids has allowed utilities and customers to communicate in both directions, completely changing the way power is distributed. Compared to standard metres, smart metres as an essential part of Advanced Metering Infrastructure (AMI) offer a more precise and detailed picture of energy usage by providing real-time data on patterns of electricity consumption, [3]. This data can be used to train machine learning (ML) and deep learning (DL) algorithms to precisely identify electricity theft in power grids, [10].

The limitations of traditional detection methods highlight the critical need for more sophisticated and automated approaches to identify electricity theft. In this regard, AI algorithms have shown promise as a potential remedy. It can analyse vast amounts of data from smart metres and identify minute irregularities that could be signs of theft [10]. Artificial intelligence methods, including deep learning algorithms, which have the ability to identify intricate patterns in past consumption data and apply them to categorise current readings as either normal or suspect. When compared to manual procedures, this automated approach can greatly increase detection efficiency and accuracy. While various ML and DL models have been explored for electricity theft detection, several limitations remain. Traditional ML methods often rely on one-dimensional (1D) consumption data, failing to capture the periodicity inherent in electricity usage patterns, [11]. Additionally, imbalanced datasets, where legitimate users significantly outnumber electricity thieves, can hinder model performance in accurately classifying the minority class (theft), [12].

DL algorithms are very good at finding patterns in large, complicated data sets, which makes them ideal for assessing the vast quantities of data produced by smart metres, [8], [12]. By processing consumption data across different time intervals, these algorithms can capture temporal patterns, consumption spikes, and other irregularities indicative of theft activities [11]. Also, the requirement for labour-and resource-intensive human feature engineering is eliminated by deep learning models' ability to automatically extract relevant features from the data [10].

The effective development and deployment of AI-driven systems for detecting electricity theft present various notable advantages for both power distribution companies and consumers:

Decreased Revenue Losses: Through precise identification of electricity theft, power distribution companies can reduce monetary losses and enhance their revenue flow. This financial gain can then be channelled into grid enhancements and growth, ultimately resulting in a more dependable and effective power provision for all consumers [2], [7].

Improved Grid Stability: Early detection of theft activities can help prevent overloading of the grid and ensure stable power supply for legitimate consumers. Unaddressed theft can lead to power outages and disruptions, impacting businesses, homes, and critical infrastructure [6].

Enhanced Efficiency: AI-based systems can automate the detection process, freeing up manpower for other critical tasks within the power distribution company. Previously, manual metre reading and inspection required a significant investment of human resources. Automating theft detection allows utilities to deploy personnel more effectively for maintenance, customer service, and grid infrastructure improvement projects [3].

Data-driven Decision Making: The insights gleaned from the model's predictions can inform more targeted and effective strategies for curbing electricity theft [13]. Utilities can use the data to identify areas with high theft prevalence and deploy targeted intervention efforts. In addition, the data can also be utilised to create consumer education programmes that emphasise the negative effects of electricity theft to the grid [13].

Despite the advancements in AI-based electricity theft detection, several challenges remain unaddressed;

Data Availability: Obtaining sufficient labelled data for training complex AI models can be a significant hurdle. Labelled data refers to data points where the consumption pattern has been categorised as either normal or indicative of theft. Due to privacy issues, utilities might be reluctant to disclose customer data. Data augmentation techniques and transfer learning can be looked into to overcome this problem, [14].

Data Privacy: Data privacy concerns are paramount when dealing with customer consumption data. Sensitive information about a consumer's daily activities can be inferred from their electricity usage patterns, [15]. Anonymization and privacy-preserving strategies must be used to guarantee adherence to applicable laws, [11].

Class Imbalance: Electricity theft data might be imbalanced, with a significant majority of readings representing normal consumption patterns and a smaller portion reflecting theft activities. This imbalance can hinder the training process of AI models [12]. This issue could be solved by

employing strategies like oversampling or under-sampling the data.

Evolving Theft Techniques: As detection methods improve, perpetrators may adopt more sophisticated theft techniques to circumvent them [11]. The AI model needs to be continuously updated and adapted to identify new and emerging theft patterns.

Several machine learning and deep learning approaches have been explored for electricity theft detection, with varying degrees of success.

2 Related Works

The detection of electricity theft has evolved significantly over the past two decades, progressing from simple meter-based detection to sophisticated AI-driven approaches. Early pioneering work by Hernandes Jr et al., in 2001 established the foundation for non-invasive theft detection by developing an electronic Ah meter device for comparing customer consumption patterns, [16]. Their comprehensive statistical study, involving over 80,000 customers in São Paulo, Brazil, demonstrated the effectiveness of consumption pattern analysis in identifying tampered or defective meters, achieving significant improvement in inspection efficiency.

Building on this statistical approach, Nagi et al., introduced one of the first applications of Support Vector Machines (SVM) for electricity theft detection in 2008. Their work with Tenaga Nasional Berhad in Malaysia demonstrated how machine learning could effectively analyse customer load profiles to expose abnormal behaviour correlated with Non-Technical Loss (NTL) activities, [17]. This marked a crucial shift towards automated classification approaches, achieving superior results compared to traditional inspection methods. Stajić et al., further contributed to this evolution by developing an interoperable smart grid platform in Serbia, emphasizing the importance of comprehensive monitoring systems in loss detection and establishing the groundwork for modern AI-based approaches, [18].

More recent developments have focused on deep learning approaches. Zheng et al., introduced a wide and deep CNN model for electricity theft detection in smart grids, [19]. Their model comprises two components: a deep CNN component for capturing nonperiodic theft patterns and a wide component for extracting global features from electricity consumption data. By leveraging 2-D data representation, their approach demonstrated superior performance in detecting theft activities compared to existing methods. Hasan et al., proposed a CNN-LSTM hybrid model tailored for smart grid data classification, [20]. LSTM architecture addresses the time-series nature of power consumption data, while CNN automates feature extraction and classification processes. Their work emphasises the importance of data pre-processing, including interpolation and outlier handling, to enhance model accuracy. Additionally, they employed synthetic data generation to mitigate class imbalance issues, achieving satisfactory results in identifying theft users. However, LSTMs can be computationally expensive to train and may require large datasets for optimal performance. Fang et al., introduced a LSTM and a modified CNN to predict electricity usage patterns and detect abnormalities, [21]. The authors extract relevant features that affect meter error, such as voltage and current readings at different intervals. They included polynomial fitting to model the error values in electricity measurements. By comparing different polynomial degrees, the authors identify the best fit for the data, which helps in understanding the underlying patterns and trends. An LSTM model with 40 neurons in the first hidden layer and using the root mean square error (RMSE) as the loss function was used. The model was trained for 1000 epochs. the authors use a sliding window approach to identify days with significant deviations between predicted and actual values. This method not only helps in detecting anomalies but also helps in identifying faulty meters that need replacement. The authors also compare different models and found that the time series recurrence plot CNN (TS-RP CNN) performs best in detecting anomalies, achieving an accuracy of about 82%. Yao et al., introduced a hybrid method, AdaBoost-CNN, combining adaptive boosting (AdaBoost) and CNN for electricity theft detection, [22]. Multiple CNN-based classifiers were trained to extract diverse features from consumption data, which were then aggregated by AdaBoost to enhance classification performance. Their experimental results, based on real smart energy data, demonstrated the superiority of the hybrid classifier over conventional methods in detecting theft activities. Singh and Venkaiah in 2023, addressed the challenge of data imbalance in theft detection by proposing a multi-layer model classifier, [23]. Their approach involves data preparation, including interpolation and outlier handling, followed by data balancing techniques such as AdaSys. A two-layer model, comprising heterogeneous machine learning models and an ANN, demonstrated improved performance in identifying theft users on real consumption datasets. Mazid et al., proposed a hybrid approach combining principal component analysis (PCA) and CNN for power theft detection, [24]. Their method involves feature selection, extraction,

and classification stages applied to smart metre data. By leveraging optimised hyperparameters and CNN-PCA methodology, their approach achieved high accuracy rates, outperforming previous methods. Zhou et al., addressed the challenge of sparse and imbalanced data in low-voltage networks by proposing a CNN and data augmentation method for theft detection, [25]. Their approach utilises kernel density estimator (KDE) and Monte Carlo method for data expansion, followed by CNN classification. Experimental results confirmed the effectiveness of their method in achieving high performance metrics. Ibrahim et al., presented a CNN-based approach for electricity theft detection in smart grids, [26]. Their work focused on feature reduction using the Blue Monkey (BM) algorithm to enhance classifier performance. By designing high-performance signal classifiers, their approach demonstrated promising results in identifying theft activities. Dimf et al., proposed a bi-LSTM and CNN hybrid model for theft detection, incorporating various techniques such as data pre-processing, synthetic data generation, and feature selection, [27]. Their approach achieved high-quality results comparable to existing methods, highlighting the effectiveness of combining CNN and bi-LSTM architectures. Khan et al., addressed challenges in electricity theft detection using supervised learning techniques on smart metre data, [15]. Their proposed model combines Adasyn algorithm for class imbalance, VGG-16 module for feature extraction, and FA-XGBoost for classification. Simulation results demonstrated superior performance in handling large time series data and accurate theft detection. Abel et al., proposed a matrix converter-based solution to mitigate electricity theft at low distribution voltages, [28]. By focusing on frequency variation and Total Harmonic Distortion (THD), their approach aimed to eliminate metre bypassing theft, presenting a novel solution to complement smart metering systems. Ullah et al., introduced a hybrid deep neural network model combining CNN, particle swarm optimization, and gated recurrent unit for electricity theft detection, [29]. Their approach addressed issues of overfitting and data imbalance, achieving robustness, accuracy, and generalisation in theft detection tasks.

The evolution of electricity theft detection techniques reveals a clear trend toward increasingly sophisticated machine learning approaches, with particular emphasis on improving classification accuracy through hybrid models and advanced data pre-processing techniques. While early methods relied on simple statistical comparisons, modern approaches leverage deep learning architectures to capture complex patterns in consumption data. However, challenges remain in balancing computational efficiency with classification accuracy, particularly when dealing with imbalanced datasets and real-time detection requirements. These challenges present opportunities for further research in developing more efficient and accurate detection methods.

3 Methodology

This research proposes an integrated AI model that combines the strengths of CNNs and SVMs to address the limitations of existing techniques. This chapter discusses a breakdown of the proposed method. The proposed method is divided into three phases; (1) data pre-processing, (2) feature extraction, and (3) classification phase. Figure 1 shows the workflow of the proposed method.

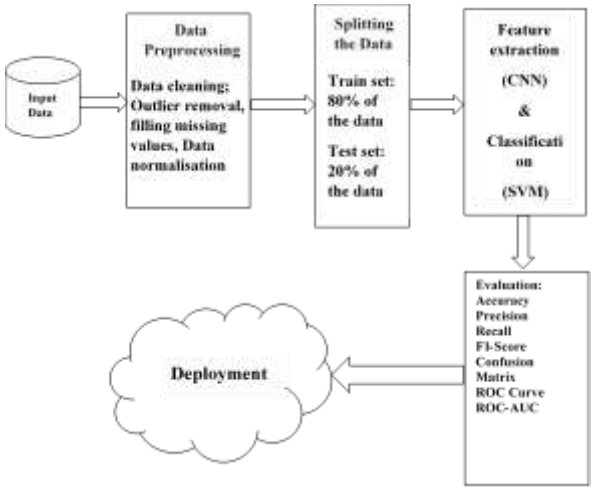

Fig. 1: Workflow of the proposed method

3.1 Data Pre-processing

The main aim of pre-processing is to verify the quality of the data to be used and to transform the data into usable format, [30], [31]. The pre-processing steps involve data cleaning (outlier removal, duplicate removal and filling of missing values) and data normalisation. Outlier removal was done by applying the IQR technique. The filling of missing values is done using the SimpleImputer method and the mean strategy. Oversampling involves replicating data points from the minority class (theft) to create a more balanced dataset. Data normalisation was done by scaling the features of the dataset to a standard range using Sklearn's StandardScaler method to ensure uniformity and prevent dominance by certain features. Data pre-processing is very important because the model's efficiency is also dependent on the quality of the data [32].

3.2 Feature Extraction

Extracting relevant features from raw data helps in improving the model's performance and accuracy. In this project feature extraction was done using CNN.

3.2.1 Detailed Feature Extraction Architecture of CNN

The feature extraction architecture of a Convolutional Neural Network (CNN) comprises several key components, including convolutional layers, pooling layers, activation functions, and fully connected layers. Each component plays a crucial role in the network's ability to learn hierarchical features from input data.

The convolutional layers consist of filters that convolve across the input data to extract features. Each filter detects patterns or features in the input data through element-wise multiplications followed by summation operations. Mathematically, the output of a convolutional layer can be expressed as:

$$Output = f(Input * Filter + b) \quad (1)$$

Where * denotes the convolution operation, f is the activation function (ReLU), and b represents the bias term, [33].

Activation functions introduce non-linearity into the network, enabling it to learn complex patterns. The Rectified Linear Unit (ReLU) is commonly used due to its computational efficiency and ability to mitigate the vanishing gradient problem:

$$\text{ReLU}(x) = \max(0, x) \quad (2)$$

Pooling layers down-sample the feature maps obtained from the convolutional layers, reducing their spatial dimensions while retaining important features, [34]. This helps in reducing computational complexity, providing a form of translation invariance, controlling, and overfitting, [34]. Common pooling operations include max pooling and average pooling.

After passing through the convolutional and pooling layers, the extracted features reside in a multi-dimensional format. The flatten layer transforms this data into a single 1D vector suitable for feeding into the next layer, [35].

The fully connected layers connect every neuron in one layer to every neuron in the next layer, enabling high-level feature learning and classification. The output of a fully connected layer can be expressed as:

$$y = f(Wx + b) \quad (3)$$

Where W is the weight matrix, x is the input vector, b is the bias vector, and f is the activation function, [33].

The output of the last fully connected layer is fed into a sigmoid activation function for binary classification into different classes, [35]:

$$\sigma(x) = \frac{1}{(1 + e^{-x})} \quad (5)$$

For multi-class classification, a softmax function may be employed, [35]. The overall CNN architecture integrates these components in a sequential manner, allowing for end-to-end learning of features and classification. Figure 2 illustrates a typical CNN architecture, showcasing the arrangement of these layers.

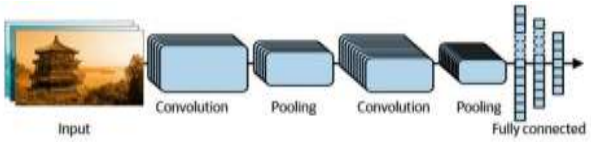

Fig. 2: Typical CNN architecture

3.3 Classification

When presented with a new data point (representing an unseen consumption sequence), the CNN extracts features and presents them to the SVM as shown in figure 3. Based on the hyperplane and the support vectors learned during training, the SVM classifies the new data point as either normal consumption or potential theft.

Fig. 3: Framework of proposed model

3.3.1 Detailed Architecture of SVM

Support Vector Machines (SVMs) are supervised learning models commonly used for classification and regression. The primary objective of SVM is to find an optimal hyperplane that maximizes the margin between two classes in a dataset, [35].

In SVM, the goal is to maximize the margin, or distance, between the separating hyperplane and the closest data points from each class. For linearly separable data, this margin maximization is formulated as a convex optimization problem, [36]. The hyperplane can be defined as:

$$f(x)=w \cdot x+b \quad (4)$$

where w is the weight vector, and b is the bias term. The optimization goal for a hard-margin SVM is to minimize the norm $\|w\|^2$, which directly maximizes the margin. This leads to the primal optimization problem:

$$\min_{\omega,b,\varepsilon} \frac{1}{2}||\omega||^2 + C\sum_{i=1}^{N}\varepsilon \quad (5)$$

Solving SVMs in their dual formulation often simplifies computations, especially with high-dimensional data. The dual formulation uses Lagrange multipliers α_i to reformulate the objective in terms of dot products between input vectors, which enables the kernel trick. The kernel trick allows SVMs to implicitly compute the dot product in the higher-dimensional feature space without explicitly transforming the data, [37]. This makes SVMs computationally efficient for high-dimensional data. The dual problem is given by:

$$\max_{\alpha}\sum_{i=1}^{N}\alpha_i - \frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N}\alpha_i\alpha_j y_i y_j (x_i \cdot x_j) \quad (6)$$

subject to:

$$0 \le \alpha_i \le C, = \sum_{i=1}^{N}\alpha_i y_i = 0 \quad (7)$$

This dual form allows us to apply kernel functions, which compute dot products in a high-dimensional feature space without explicitly transforming the data, reducing computational complexity.

Kernel functions are used by SVMs to transform input data into higher-dimensional feature spaces, where linear separation becomes possible [35]. Common kernel functions include:

- Linear kernels: Suitable for linearly separable data and high-dimensional spaces.
- Polynomial kernels: Useful for data with complex relationships.
- Radial basis function (RBF) kernels: Effective for non-linearly separable data.
- Sigmoid kernels: It is used as an alternative to the RBF kernel, often used in neural networks; less commonly applied in SVMs.

To handle complex data distributions, SVM employs a non-linear mapping that transforms the input data into a high-dimensional feature space. In this feature space, a linear decision boundary can be identified, which corresponds to a non-linear boundary in the original input space, [37]. By using kernel functions, SVM avoids the computational cost of explicitly mapping data, making it both efficient and powerful for non-linear data [35].

In summary, SVMs are effective in high-dimensional and non-linear settings due to the combination of kernel functions, dual formulation, and support vector optimization, providing an adaptable solution for tasks like electricity theft detection. This adaptability enables SVMs to classify data accurately by maximizing the margin between classes, thus ensuring robust performance across various applications. Figure 4 presents the SVM classification architecture.

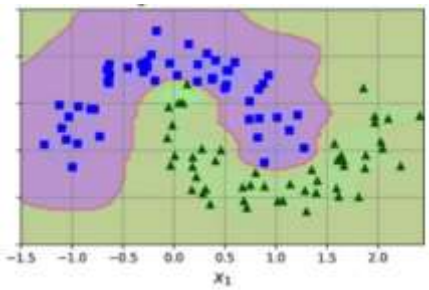

Fig. 4: SVM classification architecture

3.4 Model Evaluation

After training, the integrated model underwent evaluation to assess its performance in detecting electricity theft.

Various performance metrics such as accuracy, precision, recall, F1-score, and ROC-AUC were used to measure the model's effectiveness in distinguishing between normal and theft activities. The equation of accuracy, precision, recall and f1-score are given below.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (3)$$

$$Precision = \frac{TP}{TP + FP} \quad (4)$$

$$Recall = \frac{TP}{TP + FN} \quad (5)$$

$$F1 - score = 2 * \frac{Precision * Recall}{Precision + Recall} \quad (6)$$

A confusion matrix was generated to visualise the model's classification results and identify any

misclassifications or errors. Confusion matrix divides the dataset into four basic segments: true positive (TP), false positive (FP), true negative (TN) and false negative (FN), [38]. TP and TN show the correctly predicted positive and negative samples whilst FP and FN show the falsely classified negative samples as positive and positive samples as negative, respectively, [38]. ROC curve which analyses the trade-off between true positive rate and false positive rate was also plotted. The true positive rate and false positive rate are expressed below.

$$True\ Positive\ Rate(TPR) = \frac{TP}{TP + FN} \quad (7)$$

$$False\ Positive\ Rate(FPR) = \frac{FP}{FP + TN} \quad (8)$$

3.5 Deployment

The model was deployed to the cloud using a Python web framework, Streamlit, after satisfactory evaluation and hyperparameter tuning. Streamlit is an open source Python for building interactive web applications and for easy deployment of machine learning models.

4 Result

The model's performance is demonstrated by the experimental results. We evaluated the performance with different performance metrics. The model's performance was compared to the performance of other machine learning models using the same dataset.

4.1 Experimental Results

Using evaluation measures like accuracy, recall, precision, F1-score, and ROC AUC score, we assessed the effectiveness of the proposed approach. The percentage of all subjects that were correctly classified is referred to as accuracy. Recall is the percentage of those who test positive and actually have the condition. The number of the subjects accurately classified as positive out of all those classified as positive is known as precision. A harmonic mean of recall and precision is the F1-score. ROC AUC score shows how well the classifier distinguishes positive and negative classes. Table 1 shows the performance score of the model for different metrics.

Table 1. Performance of Proposed model

Metric	Score
Accuracy	0.966
Recall	0.961
Precision	0.972
F1	0.966
ROC AUC	0.976

Table 1 shows the performance score of our proposed model for different metrics. As shown, the model achieves high scores across all metrics, with an accuracy of 0.966 and a ROC-AUC of 0.976, indicating strong overall performance and discriminative ability.

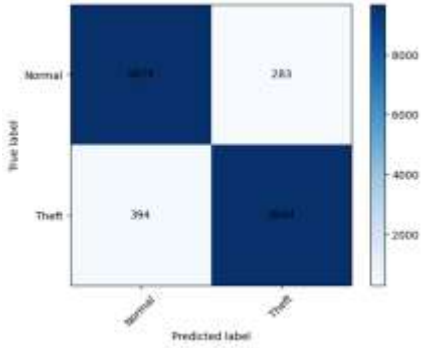

Fig. 5: Confusion Matrix of test set prediction result of proposed model

The classification results of the model proposed from the figure 5, which is the confusion matrix are as follows: the number of TPs, FNs, FPs, and TNs is 9679, 283, 394, and 9644, respectively. Figure 6 shows the roc curve.

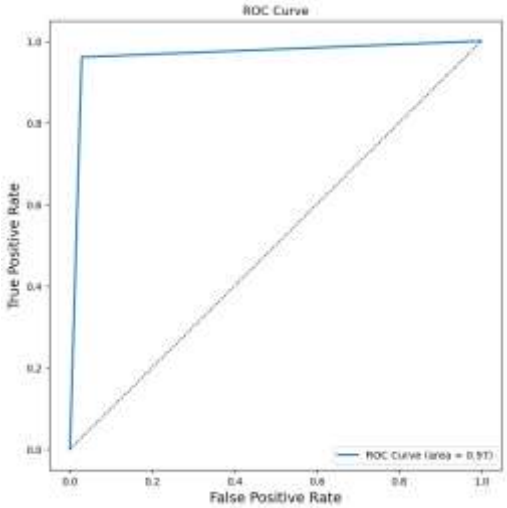

Fig. 6: ROC curve of proposed model

4.2 Comparative Analysis

To evaluate the effectiveness of our proposed hybrid CNN-SVM model, we conducted a comprehensive comparative analysis against several state-of-the-art machine learning and deep learning models. Table 2 presents the ROC AUC scores for different methods, while Figure 7 illustrates the performance metrics across all comparative experiments.

Table 2. Performance comparison with other models

Model	**ROC AUC score**
CNN-SVM	0.976
CNN	0.94
SVM	0.89
XGB	0.964
RF	0.962
DT	0.951
LR	0.963

As evident from Table 2, our proposed CNN-SVM model achieves the highest ROC AUC score of 0.976, outperforming all other models. The next best performer is XGB (Extreme Gradient Boosting) with a ROC-AUC of 0.964, followed closely by LR (Logistic Regression) at 0.963 and RF (Random Forest) at 0.962. The standalone CNN and SVM models show lower performance with ROC AUC scores of 0.94 and 0.89, respectively.

Figure 7 provides a more detailed comparison across multiple performance metrics

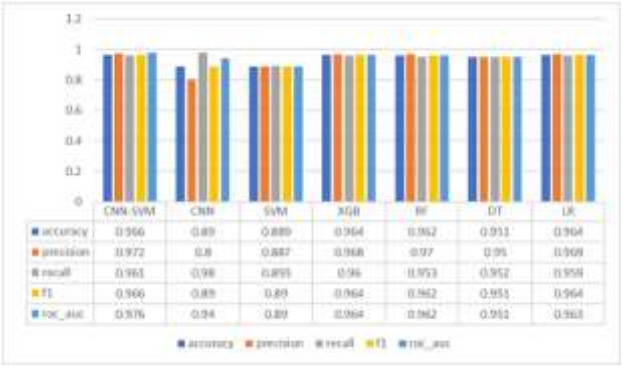

Fig. 7: Comparison with other models

The superior performance of the proposed CNN-SVM model is evident across all metrics. It achieves the highest scores in accuracy (0.966), precision (0.972), F1 score (0.966), and ROC AUC (0.976). The model's recall (0.961) is slightly lower than the standalone CNN (0.98), but this is compensated by its significantly higher precision, resulting in a better overall F1 score.

The effectiveness of our hybrid approach is further emphasised when comparing it to the standalone CNN and SVM models. The CNN-SVM model outperforms both in all metrics except recall, where the standalone CNN shows a marginally higher score. This suggests that the hybrid model successfully leverages the strengths of both techniques while mitigating their individual weaknesses.

Among the traditional machine learning models, XGB and LR show competitive performance, particularly in terms of accuracy and ROC AUC. However, they fall short of the CNN-SVM model across all metrics. The Decision Tree (DT) model shows the lowest performance among the compared models, indicating its limitations in capturing the complex patterns inherent in electricity theft data.

4.3 Web Application

An intuitive interface for non-technical users in utility companies was developed to allow them to easily interpret and act on the model's outputs. Figure 8, shows the home page which contains the fields where the user is expected to input. After the user puts in the relevant inputs and clicks the predict button the result is shown which is either figure 9, for theft detected, and figure 10, for a normal user.

Fig. 8: Home page

Fig. 9: Theft Detected

Fig. 10: Normal user

4.4 Discussion

Accuracy, recall, precision, f1-score, ROC-AUC score, and confusion matrix, which summarise the prediction outcomes on the test data, were used to assess the performance of the proposed model. On the test data, the suggested model outperformed other machine learning models like CNN-SVM, CNN, SVM, XGB, RF, DT, and LR, achieving an accuracy of 0.966. In comparison to these models, the proposed model had higher recall, precision, f1-score, and ROC-AUC score.

The results of this study indicate that the proposed CNN-SVM hybrid model is an efficient approach for electricity theft detection, offering improvements in both accuracy and reliability.

The web application's interface makes it easy for non-technical users in utility companies to easily interpret and act on the model's outputs.

5 Conclusion and Future Work

The proposed CNN-SVM hybrid model addresses the significant energy and financial losses caused by electricity theft and consumer misuse. This approach not only promises to reduce non-technical losses for utility companies but also encourages more efficient electricity usage among consumers.

Our integrated CNN-SVM model demonstrated superior performance compared to traditional machine learning approaches in detecting electricity theft. By synergizing the feature extraction capabilities of CNNs with the robust classification strength of SVMs, we achieved higher accuracy, precision, and recall. The CNN component proved particularly effective in automatically extracting relevant features from raw consumption data, while the SVM classifier excelled in discriminating between legitimate consumption patterns and fraudulent activities. This resulted in a lower false positive rate, crucial for practical implementation in real-world scenarios.

The model can be integrated into smart grid systems for real-time monitoring and detection of anomalies in electricity consumption patterns. Utility companies can use this system to identify potential theft cases, thereby protecting their revenue streams. The model's insights can help in understanding and predicting consumer behaviour, leading to improved energy management strategies. The system can assist in ensuring compliance with energy regulations by detecting unusual consumption patterns that may indicate non-compliance.

This research demonstrates the effectiveness of combining deep learning (CNN) with traditional machine learning (SVM) for complex pattern recognition tasks. The success of our model in extracting features from electricity consumption data advances the field of automated feature learning in time series analysis. Our approach shows how AI can be scaled to handle large-scale, real-world problems in the energy sector.

The CNN-SVM model can be further enhanced by integrating it with other AI technologies. Incorporating Reinforcement Learning algorithms could allow the model to adapt and improve its detection capabilities over time based on feedback from real-world implementations. Implementing explainable AI techniques could make the model's decisions more interpretable, increasing trust and adoption among stakeholders. Also, federated Learning could enable multiple utility companies to collaboratively train the model without sharing sensitive data, enhancing its generalisation capabilities.

Future research directions for this project are varied and promising. To further enhance the model's capabilities, incorporating data from smart metres, weather patterns, and socio-economic indicators could provide valuable contextual insights, leading to improved detection accuracy. Another critical area of focus is ensuring the model's resilience against adversarial attacks, which is crucial for high-stakes applications where reliability is paramount. Additionally, exploring the model's adaptability to different geographical regions and energy consumption patterns through transfer learning techniques could significantly broaden its applicability. Investigating the feasibility of deploying lightweight versions of the model on edge devices would enable real-time, on-site detection, making the system even more efficient. Lastly, addressing potential biases in the model and ensuring fair treatment across different consumer demographics is essential for maintaining a just and equitable solution. By pursuing these research

directions, the model can become even more effective, robust, and widely applicable, ultimately driving progress in electricity theft detection and contributing to a more sustainable energy future.

In conclusion, while our CNN-SVM hybrid model shows significant promise in addressing the critical challenge of electricity theft, continued research and development are necessary. Future work should focus on enhancing the model's adaptability, interpretability, and ethical implementation. As we advance, the integration of this technology with broader smart grid initiatives and energy management systems could lead to more efficient, secure, and sustainable energy ecosystems. The potential impact extends beyond theft detection, potentially revolutionising how we understand and manage energy consumption in an increasingly connected world.

References:

[1] Shehzad, F., Javaid, N., Almogren, A., Ahmed, A., Gulfam, S. M., & Radwan, A. A robust hybrid deep learning model for detection of non-technical losses to secure smart grids. *IEEE Access*, *9*, 128663-128678, 2021.

[2] Henriques, H. O., Corrêa, R. L. S., Fortes, M. Z., Borba, B. S. M. C., & Ferreira, V. H. (2020). Monitoring technical losses to improve non-technical losses estimation and detection in LV distribution systems. Measurement, 161, 107840.

[3] Marques, L., Silva, N., Miranda, I., Rodriges, E., & Leite, H. (2016). Detection and localisation of nontechnical losses in low voltage distribution networks.

[4] Onat, N. E. V. Z. A. T. (2010). Techno-economic analysis of illegal electricity usage in Turkey and policy proposals. WSEAS Transactions on Power Systems, 3(5), 213-222.

[5] Messinis, G. M., & Hatziargyriou, N. D. Review of non-technical loss detection methods. *Electric Power Systems Research*, *158*, 250-266, 2018.

[6] Tsado, J., & Abel, S. (2022). Electricity Theft Mitigation at Low Voltage Distribution End Using Indirect Matrix Converter.

[7] OLADOSU, D. (2024). Energy Theft Detector (ETD): A Salvage Module from Meter Bypassing and Illegal Tapping of Electricity.

[8] Nirmal, S., Patil, P., & Kumar, J. R. R. (2024). CNN-AdaBoost based hybrid model for electricity theft detection in smart grid. *e-Prime-Advances in Electrical Engineering, Electronics and Energy*, *7*, 100452.

[9] Saeed, M. S., Mustafa, M. W., Hamadneh, N. N., Alshammari, N. A., Sheikh, U. U., Jumani, T. A., ... & Khan, I. (2020). Detection of non-technical losses in power utilities—A comprehensive systematic review. *Energies*, *13*(18), 4727.

[10] Siniosoglou, I., Radoglou-Grammatikis, P., Efstathopoulos, G., Fouliras, P., & Sarigiannidis, P. (2021). A unified deep learning anomaly detection and classification approach for smart grid environments. *IEEE Transactions on Network and Service Management*, *18*(2), 1137-1151.

[11] Liu, X., Ding, Y., Tang, H., & Xiao, F. (2021). A data mining-based framework for the identification of daily electricity usage patterns and anomaly detection in building electricity consumption data. *Energy and Buildings*, *231*, 110601.

[12] Promper, C., Engel, D., & Green, R. C. (2017, November). Anomaly detection in smart grids with imbalanced data methods. In *2017 IEEE symposium series on computational intelligence (SSCI)* (pp. 1-8). IEEE.

[13] Kim, S., Sun, Y., Lee, S., Seon, J., Hwang, B., Kim, J., ... & Kim, J. (2024). Data-Driven Approaches for Energy Theft Detection: A Comprehensive Review. *Energies*, *17*(12), 3057.

[14] Shorten, C., & Khoshgoftaar, T. M. A survey on image data augmentation for deep learning. *Journal of big data*, *6*(1), 2019,1-48.

[15] Khan, Z. A., Adil, M., Javaid, N., Saqib, M. N., Shafiq, M., & Choi, J. G. (2020). Electricity theft detection using supervised learning techniques on smart meter data. *Sustainability*, *12*(19), 8023.

[16] Hernandes Jr, L. J., Duarte, L. C., Morais, F. O., Ferreira, E. C., & Siqueira, J. A. (2001). Optimizing the inspection routine for the detection of electrical energy theft in aes eletropaulo in são paulo, brazil. WSEAS Transactions on Power Systems, 7(2), 81-89.

[17] Nagi, J., Mohammad, A. M., Yap, K. S., Tiong, S. K., & Ahmed, S. K. (2008, December). Non-technical loss analysis for detection of electricity theft using support vector machines. In 2008 IEEE 2nd International Power and Energy Conference (pp. 907-912). IEEE.

[18] Stajić, Z., Janjić, A., & Simendić, Z. (2011, July). Power quality and electrical energy losses as a key drivers for smart grid platform development. In Proceedings of the 15th WSEAS International Conference on Systems,

"Recent Researches in System science", Corfu Island, Greece, July (pp. 14-16).

[19] Zheng, Z., Yang, Y., Niu, X., Dai, H. N., & Zhou, Y. (2017). Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids. IEEE Transactions on Industrial Informatics, 14(4), 1606-1615.

[20] Hasan, M. N., Toma, R. N., Nahid, A. A., Islam, M. M., & Kim, J. Electricity theft detection in smart grid systems: A CNN-LSTM based approach. *Energies*, 12(17), 3318, 2019.

[21] Fang, J., Liu, F., Su, L., & Fang, X. (2024). Research on Abnormity Detection based on Big Data Analysis of Smart Meter. WSEAS Transactions on Information Science and Applications, 21, 348-360.

[22] Yao, Y., Hui, H., Liang, Z., Feng, X., & Guo, W. AdaBoost-CNN: A hybrid method for electricity theft detection. 2021 6th *Asia Conference on Power and Electrical Engineering (ACPEE)*, 436-440, 2021.

[23] Singh, S., & Venkaiah, C. Multi-layer model classifier for cyberattack detection in smart electric grid. 2023 5th *International Conference on Energy, Power and Environment: Towards Flexible Green Energy Technologies (ICEPE),* 1-6, 2023.

[24] Mazid, A. A., Manaullah, M., & Kirmani, S. A hybrid approach based on principal component analysis and convolution neural network for power theft detection. 2023 *International Conference on Recent Advances in Electrical, Electronics & Digital Healthcare Technologies (REEDCON),* 313-317, 2023.

[25] Zhou, Y., Zhang, X., Tang, Y., Mu, Z., Shao, X., Li, Y., & Cai, Q. (2021, July). Convolutional neural network and data augmentation method for electricity theft detection. In *2021 IEEE/IAS Industrial and Commercial Power System Asia (I&CPS Asia)* (pp. 1525-1530). IEEE.

[26] Ibrahim, N. M., Al-Janabi, S. T., & Al-Khateeb, B. Electricity-theft detection in smart grid based on deep learning. *SSRN Electronic Journal,* 202,. https://doi.org/10.2139/ssrn.3915286

[27] Dimf, G. P., Kumar, P., & Joshua, K. P. CNN with BI-LSTM electricity theft detection based on Modified Cheetah Optimization Algorithm in deep learning, 2023.

[28] Abel, S., Tsado, J., & Tola, O. J. Mitigation of electricity theft at low distribution voltage end using matrix converter. In 2022 5th *Information Technology for Education and Development (ITED)* (pp. 1-5). IEEE, November, 2022.

[29] Ullah, A., Javaid, N., Yahaya, A. S., Sultana, T., Al-Zahrani, F. A., & Zaman, F. A hybrid deep neural network for electricity theft detection using intelligent antenna-based smart meters. *Wireless Communications and Mobile Computing*, 2021, 1-19. https://doi.org/10.1155/2021/6612165

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

[31] Munawar, S., Asif, M., Kabir, B., Pamir, Ullah, A., & Javaid, N. Electricity theft detection in smart meters using a hybrid Bi-directional GRU Bi-directional LSTM model. *In Complex, Intelligent and Software Intensive Systems: Proceedings of the 15th International Conference on Complex, Intelligent and Software Intensive Systems (CISIS-2021)* (pp. 297-308). Springer International Publishing, 2021.

[32] Petrlik, I., Lezama, P., Rodriguez, C., Inquilla, R., Reyna-González, J. E., & Esparza, R. Electricity Theft Detection using Machine Learning. *International Journal of Advanced Computer Science and Applications,* 13(12), 2022.

[33] Ahmad, I. S., Zhang, S., Saminu, S., Wang, L., Isselmou, A. E. K., Cai, Z., ... & Kulsum, U. (2021). Deep learning based on CNN for emotion recognition using EEG signal. WSEAS Transactions on Signal Processing, 17, 28-40.

[34] Agrawal, V., Goswami, P. K., & Sarma, K. K. (2021). Week-ahead Forecasting of Household Energy Consumption Using CNN and Multivariate Data. WSEAS Trans. Comput, 20, 182-188.

[35] Aurélien Géron. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow (Third Edition). O'Reilly Media, Inc, 2022.

[36] Serrat, A., & Benyettou, M. (2019). ATNN and SVM for Autonomous Mobile Robot. Énternational Journal of Electrical Engineering and Computer Science (EEACS), 1, 84-89.

[37] SHIRLY, A. D., SUGANYADEVI, M., RAMYA, R., ADAIKALAM, I. A. D., & MUTHUKUMAR, P. Computation of an Effective Hybrid DFA-SVM Approach Aimed at Adaptive PV Power Management.

[38] Bhardwaj, N., Sood, M., & Gill, S. (2024). Design of Transfer Learning based Deep CNN Paradigm for Brain Tumor Classification. WSEAS Transactions on Biology and Biomedicine, 21, 162-169.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare.