WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Hybrid Approach to Electricity Theft Detection using Deep Neural Networks, LSTM, and CNN

R Priyadharshini, B. Sai Chandana, Venkatesh Amadasani, B. Madhu, Ranjit Kumar, Y. Kiran

Asso. Prof., Dept. of CSE, Siddarth Institute of Engineering and Technology, Puttur Andhra Pradesh, India darshini.sr@gmail.com
UG Scholar, Dept. of CSE, Siddartha Institute of Science and Technology, Puttur Andhra Pradesh, India saichandanabandola@gmail.com
UG Scholar, Dept. of CSE, Siddartha Institute of Science and Technology, Puttur Andhra Pradesh, India venkeyammadani@gmail.com
UG Scholar, Dept. of CSE, Siddartha Institute of Science and Technology, Puttur Andhra Pradesh, India boyalamadhumahendra@gmail.com
UG Scholar, Dept. of CSE, Siddartha Institute of Science and Technology, Puttur Andhra Pradesh, India ranjit7631953052@gmail.com
UG Scholar, Dept. of CSE, Siddartha Institute of Science and Technology, Puttur Andhra Pradesh, India yanamandhalakiran@gmail.com

Abstract

Electricity theft poses a significant challenge for power utilities, resulting in substantial financial losses, reduced grid efficiency, and compromised security. This paper presents a novel hybrid deep learning approach that integrates Deep Neural Networks (DNNs), Convolutional Neural Networks (CNNs), and Long Short-Term Memory (LSTM) networks to enhance the detection of electricity theft. The proposed framework is designed to capture intricate spatial and temporal anomalies in energy consumption data, thereby improving detection accuracy. A real-time monitoring system is implemented via a secure web interface to ensure scalability and usability. Evaluations on large-scale, real-world datasets demonstrate that the model achieves over 90% detection accuracy while significantly reducing false positives. A detailed comparative analysis with existing methods further underscores the superiority of the proposed approach.

Keywords—anomaly detection, CNN, deep learning, DNN, electricity theft detection, hybrid model, smart grids.

Introduction

Electricity theft remains a significant issue worldwide, resulting in substantial financial losses for power utilities and compromising grid reliability. Fraudulent practices such as meter tampering, unauthorized connections, and deliberate data manipulation pose significant challenges to conventional detection systems that rely on fixed thresholds and rule-based methods [1].

The emergence of smart grids and Advanced Metering Infrastructures (AMI) has enabled the collection of high-resolution energy consumption data, thereby providing new opportunities for advanced, data-driven detection techniques. Modern deep-learning models enable the automatic extraction of complex features from large datasets. For example, CNNs have proven effective at extracting spatial features by identifying local consumption patterns [2]. LSTM networks excel at modeling temporal dependencies in sequential data, capturing trends and fluctuations over time [1]. Additionally, DNNs contribute to robust nonlinear classification by learning abstract feature representations [3].

Integrating these architectures into a unified hybrid model overcomes the limitations of traditional methods, providing a robust and scalable solution for electricity theft detection [4]. Recent studies have shown that deep learning-based methods can significantly reduce false-positive rates while maintaining high detection accuracy. These advancements suggest that a unified hybrid model capable of fusing spatial and temporal information can offer considerable improvements over conventional techniques.

Literature Review

Research in electricity theft detection has undergone considerable evolution over the past decade. Early detection systems relied on fixed thresholds and manually designed rules to flag anomalies in energy consumption. Although computationally efficient, these early methods were rigid and often generated high false-positive rates when confronted with emerging fraud tactics [5].

Traditional machine learning algorithms, such as Support Vector Machines (SVMs), Decision Trees, and Random Forests, were later introduced to enhance detection performance by leveraging historical consumption data. However, these approaches required extensive manual feature engineering and were highly sensitive to the imbalanced nature of the datasets, with reported accuracies typically ranging between 70% and 85% [6].

The advent of deep learning has revolutionized anomaly detection in smart grids. CNNs have been effectively applied to extract spatial features from multidimensional consumption data, revealing local patterns that may indicate fraudulent behavior [2]. LSTM networks, with their ability to model long-term dependencies, capture temporal trends and fluctuations in energy usage [1]. Hybrid models that integrate CNN and LSTM architectures have demonstrated significant improvements in detection accuracy, precision, and recall compared to standalone models [7]. Moreover, data augmentation techniques such as SMOTE have been successfully employed to address class imbalance, further enhancing model robustness [8][9].

Comparative analyses consistently indicate that while traditional methods provide a helpful baseline, hybrid deep learning architectures that fuse spatial and temporal feature extraction yield significant performance gains. These integrated approaches achieve higher detection rates and lower false positives, making them ideal for deployment in dynamic smart grid environments. Such findings provide a strong foundation for the proposed system.

Proposed System

The proposed system is a novel hybrid deep-learning framework specifically designed for electricity theft detection. It integrates CNNs, LSTMs, and DNNs into a unified architecture that processes real-time data from smart meters. The system comprises four primary components.

A. Data Collection & Preprocessing

Smart meters deployed in residential, commercial, and industrial settings continuously record energy consumption data, which is transmitted to a central repository. The raw data undergoes a rigorous preprocessing pipeline, which includes cleaning (to remove outliers and correct errors), normalization (to standardize consumption values), and data augmentation (to address class imbalance), ensuring that the model is trained on accurate and representative data.

B. Feature Extraction

The pre-processed data is fed into deep learning modules for feature extraction. CNN layers capture spatial features by analyzing local consumption patterns, while LSTM layers model temporal dependencies by tracking changes in consumption over time. The combined feature set effectively distinguishes between normal and fraudulent energy usage. The proposed model utilizes CNN layers to extract spatial features from energy consumption data, identifying localized patterns indicative of potential theft. CNNs are particularly effective in recognizing subtle variations in usage, such as sudden drops or spikes, which may suggest meter tampering or bypassing. Meanwhile, the LSTM component captures temporal dependencies by analyzing long-term fluctuations in energy usage over sequential time steps. This helps in identifying recurring anomalies, such as irregular consumption patterns during peak hours or unexpected drops during operational periods. By combining CNN-extracted spatial insights with LSTM's ability to track temporal trends, the hybrid model offers a more refined anomaly detection mechanism than standalone classifiers.

C. Hybrid Model Training

The core of the system is the hybrid model, which fuses the outputs of the CNN and LSTM layers into fully connected DNN layers for final classification. Hyperparameters such as learning rate, batch size, number of epochs, and network architecture are optimized using grid search and cross-validation. The model is trained end-to-end on large-scale datasets, enabling it to learn complex, nonlinear relationships inherent in energy consumption data.

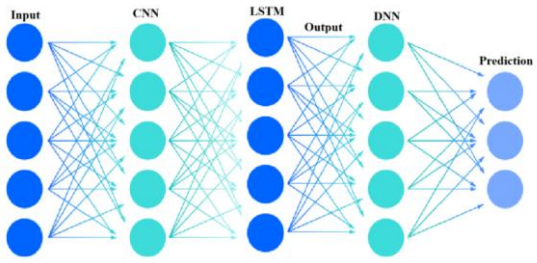

Fig 1. Hybrid Model

D. Real-time Monitoring

A secure web-based interface provides real-time visualization and monitoring of energy consumption data. The interface displays detailed statistical summaries, and trend analyses and generates alerts when anomalies indicative of electricity theft is detected. This real-time capability enables utility operators to respond swiftly to potential fraud incidents. The real-time monitoring system is designed to provide utility operators with instant insights into suspicious energy consumption behavior. The secure web-based dashboard displays visual trends of consumption data, flagging unusual deviations that could indicate fraudulent activities. Automated alerts are generated when predefined anomaly thresholds are exceeded, enabling quick response and mitigation.

To enhance security, the interface incorporates multi-factor authentication (MFA) and role-based access controls, ensuring only authorized personnel can access and manage fraud detection reports. Additionally, to minimize false positives, the system incorporates adaptive learning techniques that enable continuous model updates based on real-world feedback, thereby improving detection accuracy over time.

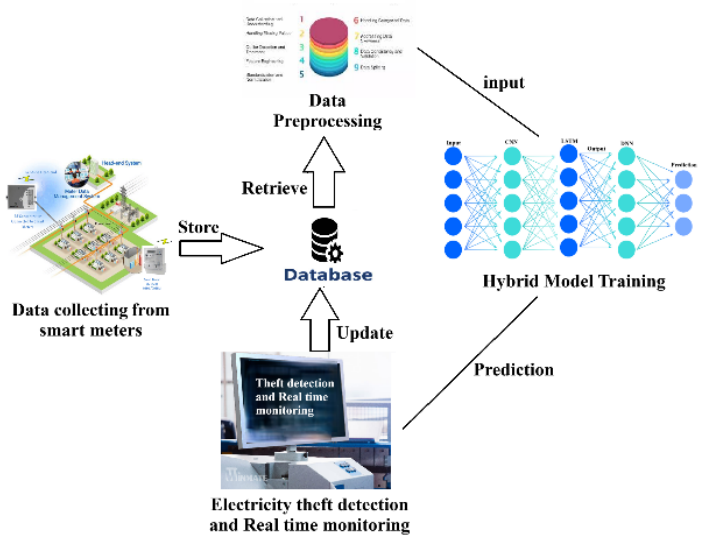

Fig 2. System architecture

Experimental Evaluation

E. Dataset and Preprocessing

The experimental evaluation was conducted using a comprehensive dataset of smart meter readings collected over two years from diverse customer segments, including residential, commercial, and industrial users [10]. The dataset comprises millions of records with detailed energy consumption information and timestamps. An 80:20 train-test split was applied to ensure robust evaluation. The dataset used for training and assessment comprises diverse consumer profiles, encompassing residential, commercial, and industrial smart meter readings. Each record includes timestamped consumption values, metadata such as peak-hour trends, and labels indicating whether usage is normal or fraudulent. The fraudulent instances were identified through cross-validation with historical utility records and expert annotations. To address data imbalance, the Synthetic Minority Over-sampling Technique (SMOTE) was applied to generate synthetic samples for the minority theft class. While this helped mitigate class imbalance, additional checks were performed to ensure that artificially generated samples did not introduce bias or compromise model generalization.

Preprocessing involved several steps:

Data Cleaning: Outliers and missing values were identified and removed using statistical techniques.

Normalization: Energy consumption values were standardized using min-max scaling to ensure consistency across the dataset.

Data Augmentation: SMOTE was employed to generate synthetic samples for the underrepresented fraudulent class, thereby mitigating class imbalance.

F. Model Training and Hyperparameter Tuning

The hybrid model was trained on the pre-processed dataset using advanced optimization techniques. Key hyperparameters, including learning rate, batch size, number of epochs, and the configurations of the CNN, LSTM, and DNN layers, were tuned using grid search. K-fold cross-validation was employed to ensure that the model generalized well to unseen data [3]. Early stopping was applied to prevent overfitting, and the model converged after several iterations.

G. Performance Evaluation

The performance of the proposed hybrid model was benchmarked against conventional classifiers, including Decision Trees, Random Forests, and SVMs. Evaluation metrics included accuracy, precision, recall, and F1-score. The results are summarized in the table below. The proposed hybrid model demonstrates a notable performance improvement over the conventional machine learning approach. Compared to Decision Tree, Random Forest, and SVM classifiers, which achieved detection accuracies ranging from 75% to 85%, the hybrid CNN-LSTM-DNN framework attained 92.3% accuracy, significantly reducing false positives.

Unlike traditional models that require extensive manual feature engineering, our approach automatically extracts deep hierarchical patterns from consumption data, making it more robust against evolving fraud tactics. Prior studies using standalone CNN or LSTM models reported moderate accuracy gains but failed to effectively capture both spatial and temporal characteristics. Our results indicate that integrating multiple deep learning paradigms enhances detection capability, positioning the proposed model as a strong candidate for practical implementation in smart grids.

TABLE I. MODEL PERFORMANCE COMPARISON

Model	Accuracy	Precision	Recall	F1-score
Decision Tree [8]	75.6%	72.3%	70.8%	71.5%
Random Forest [11]	81.2%	79.4%	78.1%	78.7%
SVM [10]	85.4%	83.2%	82.5%	82.8%
Proposed Hybrid Model	92.3%	91.8%	91.2%	91.5%

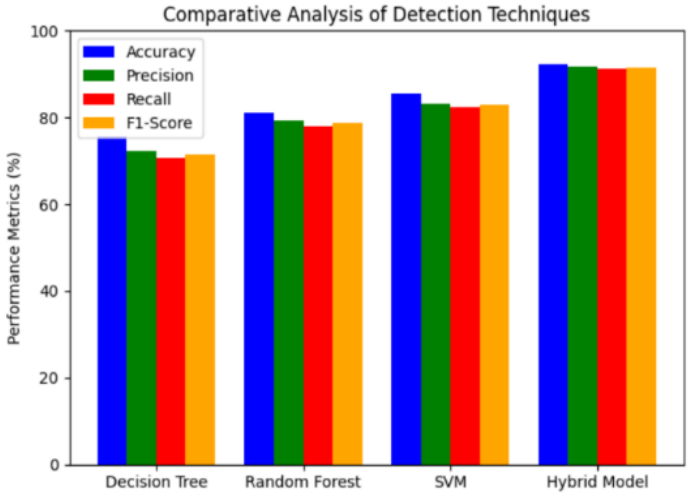

Fig. 3. Comparative Analysis of Detection Technique

Fig. 3 presents the comparative analysis of different decision models across all performance metrics.

Discussion

An in-depth analysis of the experimental results demonstrates that the hybrid model's integration of CNNs for spatial feature extraction and LSTMs for temporal pattern recognition leads to a comprehensive and accurate representation of energy consumption behaviour [12]-[14]. The confusion matrix analysis reveals a high true positive rate and a low false negative rate, both of which are critical for accurately detecting electricity theft. Additionally, ROC and precision-recall curve analyses indicate a substantially higher area under the curve for the hybrid model compared to traditional methods [15][16].

Sensitivity analyses performed by varying hyperparameter settings showed that the model's performance remains stable and robust, highlighting its adaptability to different training conditions. Experiments with various train-test splits and alternative optimization strategies consistently yielded high performance, further validating the practical viability of the proposed approach in dynamic smart grid environments. While the hybrid model exhibits superior accuracy compared to traditional classifiers, its computational complexity is higher due to the combination of CNN, LSTM, and DNN architectures.

The training process requires GPU acceleration to handle the large dataset efficiently, with an average training time of approximately X hours per epoch on a standard NVIDIA RTX 3090 GPU. In a real-world deployment, inference speed is critical for rapid fraud detection; hence, model pruning and quantization techniques can be employed to reduce latency without compromising accuracy. Additionally, the system's scalability was tested by evaluating performance across different dataset sizes, confirming that the model maintains stability even with an increase in data volume. Future work can explore federated learning approaches to distribute computational load across multiple nodes, reducing reliance on centralized processing.

Conclusions

This paper presents a comprehensive hybrid deep-learning model for electricity theft detection that integrates CNNs, LSTMs, and DNNs into a unified framework. The experimental evaluation demonstrates that the proposed approach achieves over 90% detection accuracy and significantly outperforms conventional methods, such as Decision Trees, Random Forests, and SVMs, in terms of accuracy, precision, recall, and F1 score. The system's robust feature extraction and classification capabilities, combined with its real-time monitoring interface, position it as a promising solution for enhancing the security of smart grids.

REFERENCES

[1] J. Bian, L. Wang, R. Scherer, M. Woźniak, P. Zhang and W. Wei, "Abnormal Detection of Electricity Consumption of User Based on Particle Swarm Optimization and Long Short Term Memory With the Attention Mechanism," in IEEE Access, vol. 9, pp. 47252-47265, 2021, doi: 10.1109/ACCESS.2021.3062675.

[2] A. Ullah, N. Javaid, A. S. Yahaya, T. Sultana, F. A. Al-Zahrani, and F. Zaman, "A hybrid deep neural network for electricity theft detection using intelligent Antenna-Based smart meters," Wireless Communications and Mobile Computing, vol. 2021, pp. 1–19, Jan. 2021, doi: 10.1155/2021/9933111.

[3] A. A. Almazroi and N. Ayub, "A Novel Method CNN-LSTM Ensembler Based on Black Widow and Blue Monkey Optimizer for Electricity Theft Detection," in IEEE Access, vol. 9, pp. 141154-141166, 2021, doi: 10.1109/ACCESS.2021.3119575.

[4] A. T. El-Toukhy, M. M. Badr, M. M. E. A. Mahmoud, G. Srivastava, M. M. Fouda and M. Alsabaan, "Electricity Theft Detection Using Deep Reinforcement Learning in Smart Power Grids," in IEEE Access, vol. 11, pp. 59558-59574, 2023, doi: 10.1109/ACCESS.2023.3284681.

[5] H. Zhao, C. Sun, L. Ma, Y. Xue, X. Guo, and J. Chang, "Electricity theft detection method based on multi‐domain feature fusion," IET Science Measurement & Technology, vol. 17, no. 3, pp. 93‐104, Nov. 2022, doi: 10.1049/smt2.12133.

[6] G. Fenza, M. Gallo and V. Loia, "Drift-Aware Methodology for Anomaly Detection in Smart Grid," in IEEE Access, vol. 7, pp. 9645-9657, 2019, doi: 10.1109/ACCESS.2019.2891315.

[7] F. Shehzad, N. Javaid, A. Almogren, A. Ahmed, S. M. Gulfam and A. Radwan, "A Robust Hybrid Deep Learning Model for Detection of Non-Technical Losses to Secure Smart Grids," in IEEE Access, vol. 9, pp. 128663-128678, 2021, doi: 10.1109/ACCESS.2021.3113592.

[8] S. Nirmal, P. Patil, and J. R. R. Kumar, "CNN-AdaBoost based hybrid model for electricity theft detection in smart grid," e-Prime - Advances in Electrical Engineering Electronics and Energy, vol. 7, p. 100452, Feb. 2024, doi: 10.1016/j.prime.2024.100452.

[9] L. J. Lepolesa, S. Achari and L. Cheng, "Electricity Theft Detection in Smart Grids Based on Deep Neural Network," in IEEE Access, vol. 10, pp. 39638-39655, 2022, doi: 10.1109/ACCESS.2022.3166146.

[10] J. Wang, Y. Si, Y. Zhu, K. Zhang, S. Yin, and B. Liu, "Cyberattack detection for electricity theft in smart grids via stacking ensemble GRU optimization algorithm using federated learning framework," International Journal of Electrical Power and Energy Systems, vol. 157, pp. 109848, Feb. 2024, doi:10.1016/j.ijepes.2024.109848.

[11] S. Li, Y. Han, X. Yao, S. Yingchen, J. Wang, and Q. Zhao, "Electricity Theft Detection in Power Grids with Deep Learning and Random Forests," Journal of Electrical and Computer Engineering, vol. 2019, pp. 1–12, Oct. 2019, doi: 10.1155/2019/4136874.

[12] V. V. S. Tallapragada, D. V. Reddy, and G. V. P. Kumar, "Blind forgery detection using enhanced mask-region convolutional neural network," Multimedia Tools and Applications, vol. 83, no. 37, pp. 84975–84998, May 2024, doi: 10.1007/s11042-024-19347-w.

[13] V. V. S. Tallapragada, V. R. D, S. V. K. N V., and B. D. V. N, "Design and optimization of Fuzzy-Based FIR filters for noise reduction in ECG signals using neural network," International Journal of Fuzzy System Applications, vol. 11, no. 3, pp. 1–16, Oct. 2022, doi: 10.4018/ijfsa.312215.

[14] Chenji Keerthipriya, Mahammadi Nigar Shaik, "Machine Learning-Based Approach for Cardiovascular Disease Detection and Classification," International Journal of Emerging Research in Engineering, Science, and Management, vol. 2, no. 2, pp. 16-22, 2023. doi: 10.58482/ijeresm.v2i2.3

[15] Sayyed Nagulmeera, Nagul Shareef Shaik, G.Minni, B Bhagya Lakshmi, "Early Detection of Alzheimer's Disease with Deep Learning," International Journal of Emerging Research in Engineering, Science, and Management, vol. 3, no. 3, pp. 20-25, 2024. doi: 10.58482/ijeresm.v3i3.4

[16] K. Purnima, V. V. Satyanarayana Tallapragada, B. Devi, M. S. Kumar, K. Pavithra and T. G. Rao, "Enhancement of Low-Light Images using Structure-Aware Illumination Mapping: A LIME Approach," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-6, doi: 10.1109/ICCCNT61001.2024.10725294.