REVIEW ON TEMPORAL CONVOLUTIONAL NETWORKS FOR ELECTRICITY THEFT DETECTION WITH LIMITED DATA

Usman Haruna[1], Bachcha Lal Pal[2], Ajay Sing Dhabariya[3], Faisal Rasheed[4],

Asifa Farooq Shah[5], Abbas Sani[6], Babangida Salisu Mu'azu[7],

and Abdulgaffar Abubakar Yahya[8]

Department of C.S. and Engineering, Faculty of Engineering, Mewar University, Chittorgarh, Rajasthan, India.

Emails:

[1]usmanbabany@gmail.com, [2]hodcs@mewaruniversity.co.in, [3]ajaysingh@mewaruniversity.co.in, [4]faisal@mewaruniversity.co.in, [5]asifashah@gmail.com, [6]avvassani@gmail.com, [7]babamuazu5050@gmail.com, [8]abdulgaffarabubakar40@gmail.com.

Cite this article:

Haruna U., B. L. Pal, Ajay S., Faisal R., Asifa S., S. Abbas, B. Mua'az, Abdulgaffar A. Y. (2024), Review on Temporal Convolutional Networks for Electricity Theft Detection with Limited Data. British Journal of Computer, Networking and Information Technology 7(3), 94-106. DOI: 10.52589/BJCNIT-K4PVQDAK

Manuscript History

Received: 18 Jun 2024

Accepted: 17 Aug 2024

Published: 23 Aug 2024

ABSTRACT: *Electricity theft detection using artificial intelligence (AI) and machine learning techniques have shown significant promise in recent research. However, practical implementation and widespread adoption of these advanced methods face several persistent challenges, particularly when dealing with limited data. This review delves into the computational complexity, data requirements, overfitting issues, and scalability and generalizability concerns associated with popular techniques such as Temporal Convolutional Networks (TCN), Long Short-Term Memory (LSTM), Deep Convolutional Neural Networks (DCNN), Multi-Layer Perceptron (MLP), Gated Recurrent Unit (GRU), and Artificial Neural Networks (ANN). Computational complexity and resource constraints affect the training times and convergence of TCN, LSTM, and DCNN, while high data needs and parameter tuning hinder MLP and GRU. The ANN-based method utilized by the Electricity Company of Ghana underscores overfitting and data duplication, further exacerbated by limited data availability. Moreover, the scalability and generalizability of TCN, LSTM, and DCNN across different regions and larger datasets are limited, with effectiveness varying based on electricity consumption patterns and theft tactics. Addressing these challenges through optimizing computational efficiency, improving data quality and utilization, and enhancing scalability and generalizability is crucial, especially in data-constrained environments. Continued research and development in these areas will be essential for realizing the full potential of AI-based electricity theft detection systems with limited data.*

KEYWORDS: Electricity theft detection, Artificial intelligence, Machine learning, Limited data, Computational complexity, Data quality, Scalability, Generalizability, Overfitting.

Article DOI: 10.52589/BJCNIT-K4PVQDAK
DOI URL: https://doi.org/10.52589/BJCNIT-K4PVQDAK

Introduction

Electricity plays a fundamental and pervasive role today, impacting various aspects of daily life, infrastructure, economy, and technology [1][2]. Electricity theft has become widespread in recent years and is the third most stolen item in developing countries. This has posed significant challenges to the power sector in terms of revenue generation, as it leads to increased costs for generation, transmission, and distribution companies. Furthermore, it results in higher electricity tariffs for honest customers. Electricity theft is extremely dangerous and can lead to fatal accidents, fires, electrical shocks, and power grid overloading, causing blackouts for other customers [1][2].

Many developing, underdeveloped, and economically unstable countries, such as India, Indonesia, Malaysia, Pakistan, Nigeria, Ethiopia, and China, are facing an energy crisis and are particularly affected by the nature of their distribution setup, which only records consumption readings from the meter box inside a household. This limited data can result in challenges for effectively managing energy distribution [2].

As part of ongoing efforts to reduce electricity theft, researchers have proposed several solutions to curb this challenge. However, these methods may struggle with limited data availability, especially in developing regions or new utility infrastructures [3]. This review paper investigates many papers that Mitigated ETD using Temporal Convolutional Networks (TCNs) and other models to detect electricity theft.

Electricity losses occur in two main ways: Technical Losses (TLs) and Non-Technical Losses (NTLs). Technical Losses (TLs) refer to inefficiencies in the hardware of the electrical system, such as energy dissipation in transformers and conductors. Non-technical losses NTLs) occur due to unauthorized actions like tampering with or bypassing electric meters and hacking to produce false meter readings [4][5][6]. These actions lead to abnormal electricity flow and significant data discrepancies [4]. Detecting NTLs is crucial for two key reasons. Firstly, it helps cut down on financial losses. Secondly, it enhances the reliability and security of distribution networks [2].

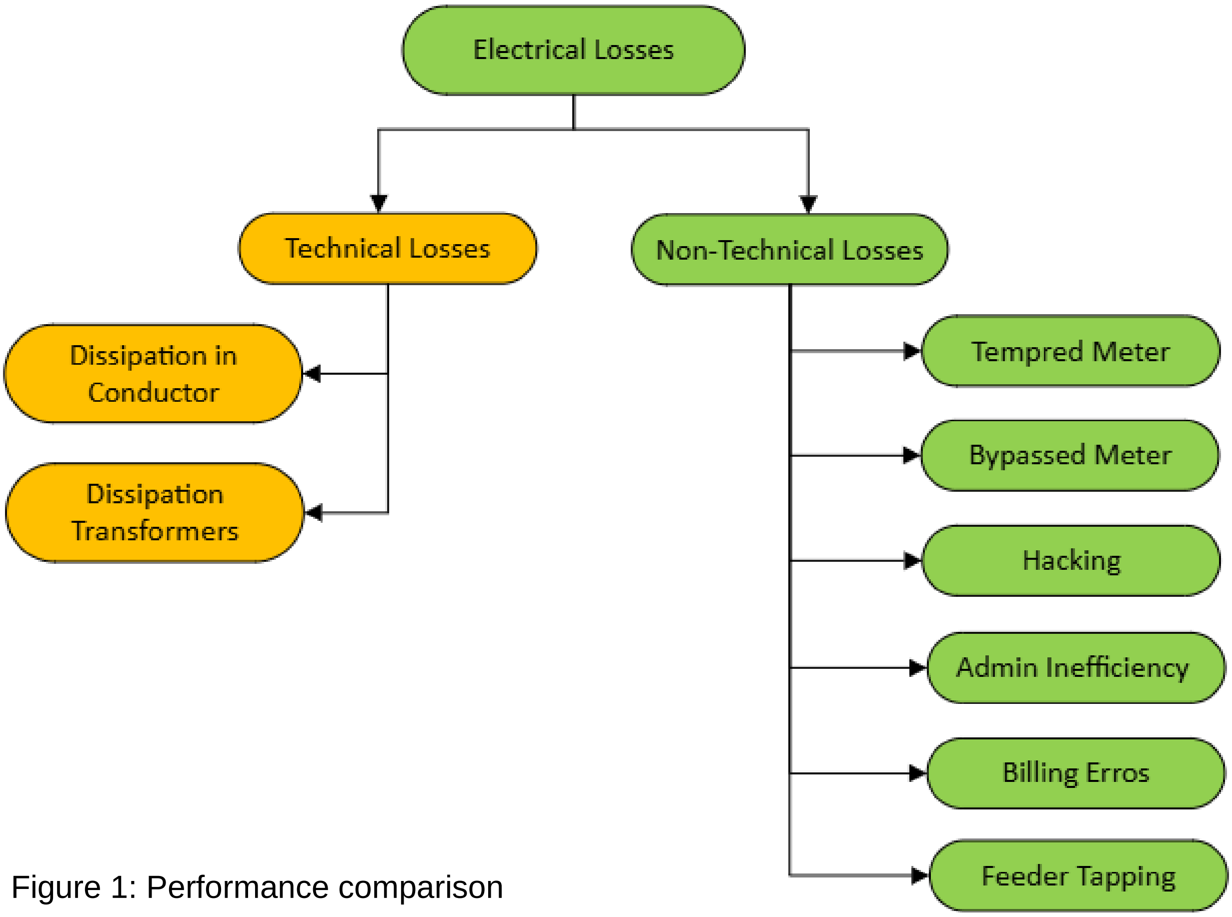


Figure 1: Performance comparison

METHOD USED IN ELECTRICITY THEFT DETECTION

Numerous methods have been proposed to address and identify illegal electricity consumption. These methods can be categorized into two main groups: State-based (Hardware) and Data-driven [7] [8]. Hardware-based methods involve the placement of sensors in relevant areas and modification of the design and architecture of smart meters to detect electricity theft, but the high operating and maintenance costs of dedicated hardware have hindered further progress in this area [7][9][10][8].

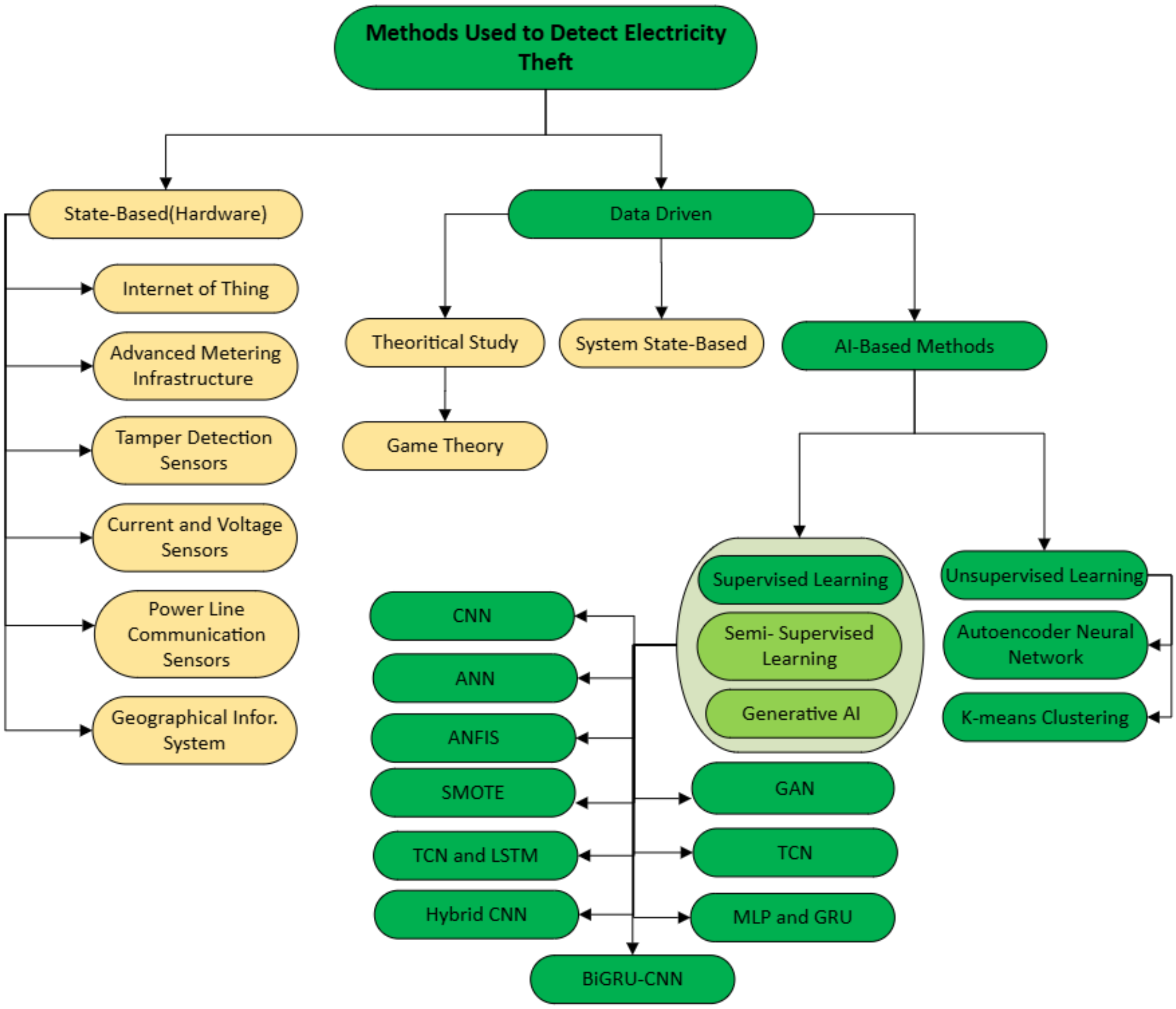
On the other hand, data-driven approaches utilize the extensive high-precision electricity consumption data generated by smart meters to identify electricity theft by consumers [7] [11]. These approaches are further divided into system state-based methods, theoretical studies using game theory and artificial intelligence-based methods, employing various algorithms and techniques such as Temporal Convolutional Networks (TCN), Long Short-Term Memory (LSTM), Hybrid Convolutional Neural Network (CNN), Artificial Neural Network (ANN), Adaptive Neuro-Fuzzy Inference System (ANFIS), and others [1] [4] [7] [11] [8].

Implementing theoretical studies and hardware solutions can be costly. Consequently, big data, AI, and optimization methods have emerged as the primary tools for decision-making, operation, and control of smart grids [12] [13].

Therefore, AI for NTL detection has the potential to become part of the standard toolbox for distribution grid controllers [5]; therefore, AI techniques for detecting electricity theft can be divided into supervised and unsupervised learning [8]. Inputs for ML algorithms can include time series data of consumption or other indicators derived from these measurements. In supervised machine learning [14] [15], it is essential to have corresponding output data for each set of input data. This implies that within the measurement database, it must be documented whether a particular consumer is honest or not [14][15]. Unsupervised machine learning, unlike supervised methods, does not rely on specific output data [8]. Instead, it can group consumers based on similar energy consumption patterns and highlight the presence of energy theft and anomalies when they occur [16].

Currently, machine learning (ML) models are implemented to identify and categorize electricity consumers as either legitimate or fraudulent [17] [18]. This approach relies on analyzing and defining the software or algorithm, which aids in predicting and detecting non-technical losses based on consumer consumption data [11][19]. ML methods or models face difficulties when dealing with highly unbalanced datasets, low-resolution data with fewer attributes, and a weak relationship between input and output classes [4][20]. Regrettably, many distribution systems in developing countries like Nigeria can only offer consumption data with low resolution, such as monthly data [3].

Article DOI: 10.52589/BJCNIT-K4PVQDAK
DOI URL: https://doi.org/10.52589/BJCNIT-K4PVQDAK



Temporal Convolutional Network (TCN)
Long Short-Term Memory (LSTM)
Hybrid Convolutional Neural Network (CNN)
Artificial Neural Network (ANN)
Adaptive Neuro-Fuzzy Inference System (ANFIS)
Hybrid system combining Multi-Layer Perceptron (MLP) and Gated Recurrent Units (GRU)
Synthetic Minority Oversampling Technique (SMOTE)
Generative Adversarial Network (GAN)
Bidirectional GRU-CNN model

Figure 2: Methods Used to Detect Electricity Theft

LITERATURE REVIEW

Artificial intelligence methods are used to apply for detecting electricity theft primarily utilizing machine learning and deep learning approaches. These techniques have been increasingly applied in recent years to address this significant problem for utility companies. In [4] A Novel Electricity Theft Detection Strategy Based on the Fusion of Dual-Time Features and Deep Learning Methods was used Utilizes a combination of Temporal Convolutional Networks (TCN), Long Short-Term Memory (LSTM), and Deep Convolutional Neural Networks (DCNN) model to extract comprehensive features from electricity consumption from SGCC and the result for accuracy 94.7%. and attained values of 0.932, 0.964, 0.948, and 0.986 for precision, recall, F1 score, and AUC, respectively.

Hybrid convolutional neural network (CNN) employed by [10], CNN for feature extraction and traditional machine learning algorithms for classification. The imbalanced dataset problem was addressed through the application of the generative adversarial network (GAN) method, highlighting the study's advancements in developing a reliable and efficient method for detecting energy theft in IoT-based smart grids.

[21] introduces artificial neural network (ANN), ANFIS, autoencoder neural network, and K-mean clustering, which is highlighted. (ANN) accurately identifies various consumer types, exhibiting a frequency error of 7.62%. In contrast, the K-means algorithm shows a slightly higher frequency error of 9.26%, while the adaptive neuro-fuzzy inference system (ANFIS) fails to detect the initial anomaly type, resulting in a frequency error of 11.11%. Comparison of the performance of these ML algorithms using statistical indicators derived from real-world energy meter measurements, used to address the critical task of detecting non-technical losses (NTLs) and energy theft within distribution networks.

To achieve electricity theft detection (ETD) in smart grids, [14] uses a hybrid system Multi-Layer Perceptron (MLP) approach with Gated Recurrent Units (GRU) to solve electricity theft using data from the Chinese National Grid Corporation (CNGC) to improve the accuracy and efficiency of detecting electricity theft by preprocessing and balancing the data before applying the models.

To address the issue of electricity theft in distribution systems, which leads to significant financial losses and operational challenges such as transformer and line overloading. The specific focus is on systems with limited data, where only consumption data is available without auxiliary information. [3] introduces a novel data pre-processing method combining statistical techniques, SMOTE, and conditional formatting to enhance the ANN's learning capabilities on data collected from the Electricity Company of Ghana, Dansoman District, Accra.

[19] addresses the problem of electricity theft in smart grids by employing a hybrid neural network model that captures customers' energy consumption patterns over multiple time scales using Bi-LSTM, and ResNet. AlexNet networks were used to address the limitations of methods that do not adequately capture the periodicity of electricity consumption or consider the temporal correlations of customers' energy usage on data obtained from the State Grid Corporation of China.

[6] proposed system uses a BiGRU-CNN model to classify electricity users as fraudulent or honest based on their consumption patterns. This classification is intended to help energy sector

companies make decisions on whether to conduct manual inspections of electricity-consuming units.

[18] addresses the challenge of accurately detecting electricity theft by consumers, which is a significant issue for power utilities by combining dual-time feature analysis with deep learning techniques. Specifically, it utilizes Temporal Convolutional Networks (TCN) and Long Short-Term Memory (LSTM) networks to extract multi-level features from electricity consumption data at different temporal scales. These features are then processed using a Deep Convolutional Neural Network (DCNN) and fed into a Fully Connected (FC) layer for classification. and they use real electricity consumption data from the State Grid Corporation of China (SGCC) to validate the effectiveness of the detection method.

[7] addresses the issue of energy theft detection (ETD) in smart grids by reviewing various methodologies for ETD, including Supervised Learning, Unsupervised Learning, Semi-Supervised Learning and Generative AI-based approaches. and emphasizes the potential of generative AI to address dataset limitations and enhance the robustness of ETD systems. These include probabilistic methods, direct distribution approximation, and diffusion-based methods.

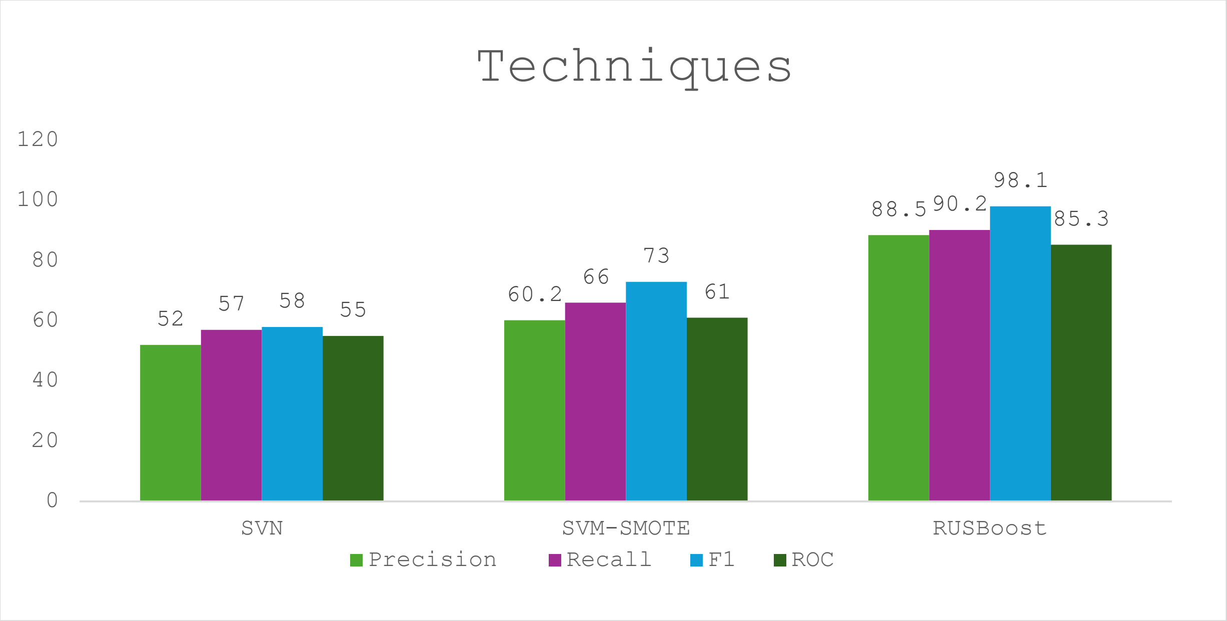


Figure 3: Performance comparison

The hardware-based solution needs a high workforce, more hardware tools, and more time needed to detect electricity theft [8]. The hardware techniques show the comparative analysis of Support Vector Machine (SVM), SVM-SMOTE, and RUSBoost. The RUSBoost has better evaluation matrices [9].

Article DOI: 10.52589/BJCNIT-K4PVQDAK
DOI URL: https://doi.org/10.52589/BJCNIT-K4PVQDAK

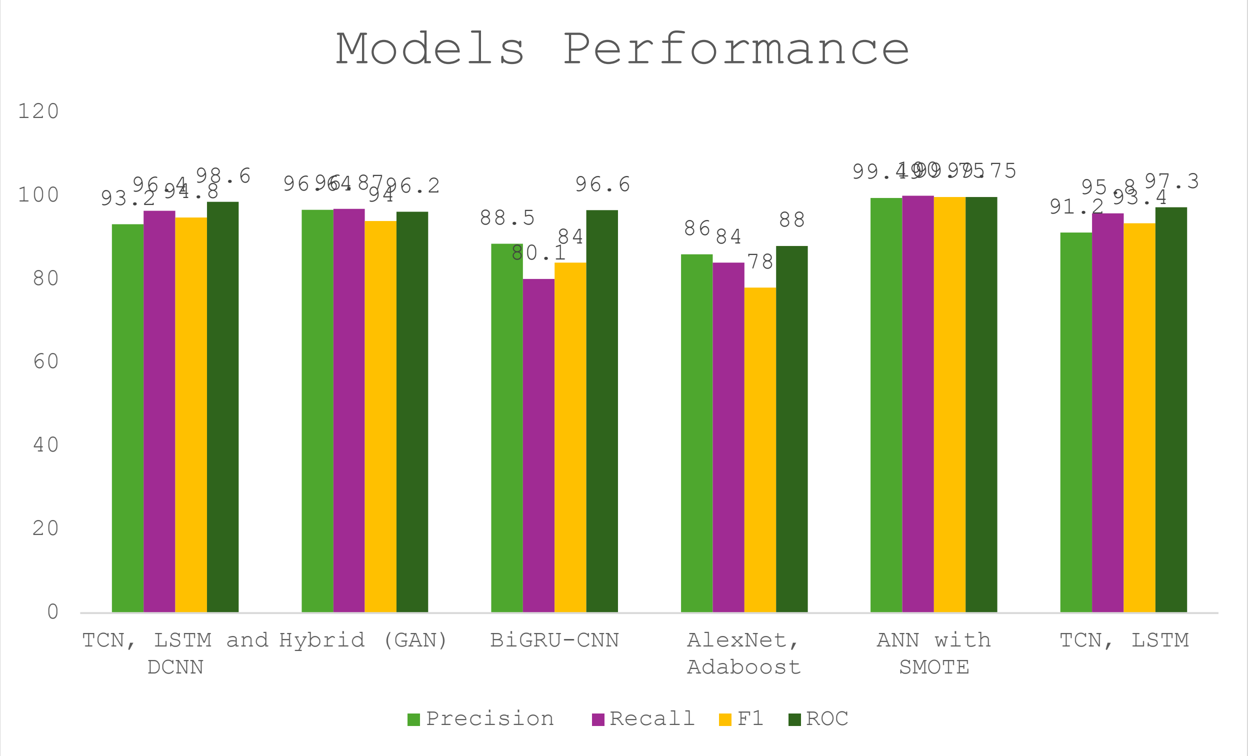


Figure 4: Performance comparison

These authors [3], [4], [6], [14], [18], [19], and [21] provide the Precision, Recall, F1 and ROC results for the TCN, LSTM and DCNN, Hybrid (GAN), BiGRU-CNN, AlexNet Adaboost ANN with SMOTE and TCN LSTM, respectively.

Article DOI: 10.52589/BJCNIT-K4PVQDAK
DOI URL: https://doi.org/10.52589/BJCNIT-K4PVQDAK

Ref.	Problem Addressed	Techniques	Data set	Accuracy	Contributions	Limitations
Huang et al 2024. [4]	A Novel Electricity Theft Detection	TCN with LSTM	SGCC	93.2	Utilizes a combination of (TCN), (LSTM), and (DCNN) to extract comprehensive features from electricity consumption data from SGC	High computational complexity and resource constraints affect training times and convergence.
Žarković et el 2024. [21]	Critical Task of Detecting Non-Technical Losses (NTLs) and Energy Theft	ANN, ANFIS, Autoencoder Neural Network, K-means Clustering	Not specified	92.38	Demonstrates the practical effectiveness of AI in identifying NTLs and energy theft, using statistical indicators from real-world energy meter measurements.	Emphasizes the need for advanced AI methodologies to improve detection accuracy and integration with current Distribution System Operator (DSO) systems.
Iftikhar et al 2024. [14]	ETD in smart grids.	hybrid system (MLP) and (GRU).	(CNGC).	93.3	Improve the accuracy and efficiency of detecting electricity theft by preprocessing and balancing the data before applying the models.	High Data Needs, Parameter Tuning and High Computational Cost
Effah et al 2023. [3]	Electricity Theft Detection with Limited Data	SMOTE for data pre-processing and ANN Based for classification	Electricity Company of Ghana, Dansoman District, Accra.	99.74	Introduces a novel data pre-processing method combining statistical techniques, SMOTE, and conditional formatting to enhance the ANN's learning capabilities	Overfitting and Data Duplication, Dependency on Consumption Data
Sun et al 2023 [19]	Electricity Theft Detection in Smart Grids	Bi-LSTM, ResNet, AlexNet and Time GAN.	SGCC	96.64	Addresses limitations in capturing periodicity and temporal correlations in electricity consumption, with synthetic data generation using Time GAN	Extensive customer electricity data is required for training; insufficient or poor-quality data can hinder accuracy.

Article DOI: 10.52589/BJCNIT-K4PVQDAK
DOI URL: https://doi.org/10.52589/BJCNIT-K4PVQDAK

Soareset el 2022. [6]	Identifying Unusual Electricity Consumption Patterns	BiGRU-CNN	Users' electrical energy consumption data.	96.6	Identifies unusual consumption patterns indicative of theft cost-effectively and efficiently.	The dataset size allowed for data removal without significant statistical impact, but missing information was discarded.
Guato Burgos et el 2024. [18]	Detecting electricity theft by consumers	(TCN) (LSTM) (DCNN)	(SGCC)	94.7	Demonstrated excellent performance with precision, recall, F1 score, and AUC values of 0.932, 0.964, 0.948, and 0.986 respectively.	Scalability across different regions and datasets is not addressed; effectiveness may vary with different consumption patterns and theft tactics.

Table 1: Comparative Analysis with Other Models

DISCUSSION

From [4], despite the promising results, the high computational complexity and resource constraints remain significant challenges. These factors can adversely affect training times and convergence, limiting the practical deployment of this method in real-world scenarios. Future research could focus on optimizing these models to reduce computational demands and improve scalability.

While demonstrating practical effectiveness, [21] emphasizes the need for advanced AI methodologies that can seamlessly integrate with current DSO systems. Future work should focus on developing more sophisticated AI algorithms that improve detection accuracy and operational efficiency.

In [14], there are high data needs, parameter tuning, and computational costs that pose significant challenges. Future research should aim at reducing these constraints, through the development of more efficient algorithms and optimization techniques.

In [3], issues such as overfitting, data duplication, and dependency on consumption data were identified as limitations. Future studies should address these challenges by exploring more robust data preprocessing methods and techniques to mitigate overfitting.

From [19], the method's reliance on extensive customer electricity data for training highlights the need for large, high-quality datasets. Insufficient data collection or poor data quality can hinder model accuracy. Future research should focus on methods to improve data quality and quantity, such as data augmentation techniques.

From [6], the data size allowed for the removal of missing information without significant statistical impact; thus, discarding data is not always ideal. Future studies should explore methods to manage missing data more effectively, ensuring the integrity and completeness of the dataset.

In [18], scalability across different regions and datasets was not addressed, and the method's effectiveness may vary with different consumption patterns and theft tactics. Future research should focus on validating the model across diverse datasets and regions to ensure its generalizability.

CONCLUSION

The studies reviewed provide valuable insights into the use of AI and machine learning techniques for electricity theft detection. While significant advancements have been made, familiar challenges such as high computational costs, data quality, scalability, and generalizability remain. Addressing these challenges through continued research and development is crucial for the practical implementation and widespread adoption of these advanced detection methods.

Computational Complexity: Techniques like TCN, LSTM, and DCNN face challenges with computational complexity and resource constraints, affecting training times and convergence.

Data Needs: Methods like MLP and GRU require high data needs, and parameter tuning, and have high computational costs.

Overfitting and Data Duplication: The ANN-based method for classification in the Electricity Company of Ghana faces issues with overfitting and data duplication.

Scalability and Generalizability: The TCN, LSTM, and DCNN methods do not address scalability across different regions or larger datasets, and their effectiveness might vary with different electricity consumption patterns and theft tactics.

REFERENCES

[1] A. Nawaz, T. Ali, G. Mustafa, S. U. Rehman, and M. R. Rashid, "A novel technique for detecting electricity theft in secure smart grids using CNN and XG-boost," *Intelligent Systems with Applications*, vol. 17, Feb. 2023, doi: 10.1016/j.iswa.2022.200168.

[2] "Electricity Theft Detection In Smart Grids Based On Deep Neural Network," 2023. [Online]. Available: www.ijcrt.org

[3] F. Effah, D. Kwegyir, E. Frimpong, M. Yaw Kwarteng, F. Boafo Effah, and E. Asuming Frimpong, "ANN-Based Electricity Theft Classification Technique for Limited Data Distribution Systems," 2023, doi: 10.25077/jnte.v12n1.1072.2023.

[4] Q. Huang *et al.*, "A Novel Electricity Theft Detection Strategy Based on Dual-Time Feature Fusion and Deep Learning Methods," *Energies (Basel)*, vol. 17, no. 2, Jan. 2024, doi: 10.3390/en17020275.

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

[6] L. D. Soares, A. de S. Queiroz, G. P. López, E. M. Carreño-Franco, J. M. López-Lezama, and N. Muñoz-Galeano, "BiGRU-CNN Neural Network Applied to Electric Energy Theft Detection," *Electronics (Switzerland)*, vol. 11, no. 5, Mar. 2022, doi: 10.3390/electronics11050693.

[7] S. Kim *et al.*, "Data-Driven Approaches for Energy Theft Detection: A Comprehensive Review," *Energies (Basel)*, vol. 17, no. 12, p. 3057, Jun. 2024, doi: 10.3390/en17123057.

[8] S. Alam, M. Ashraf, and S. Alam, "A Systematic Review on Supervised Learning Techniques in Electricity Theft Detection," *International journal of Engineering Works*, vol. 9, no. 02, pp. 22–27, Feb. 2022, doi: 10.34259/ijew.22.9022227.

[9] Dr. B. R. T. Bapu, D. J.A, S. Selvi.D, and U. S, "IOT BASED REDUCTION OF ELECTRICITY THEFT," *International Scientific Journal of Engineering and Management*, vol. 02, no. 04, Apr. 2023, doi: 10.55041/isjem00349.

[10] M. Z. Gunduz and R. Das, "Smart Grid Security: An Effective Hybrid CNN-Based Approach for Detecting Energy Theft Using Consumption Patterns," *Sensors*, vol. 24, no. 4, Feb. 2024, doi: 10.3390/s24041148.

[11] I. U. Khan, N. Javaid, C. J. Taylor, and X. Ma, "Robust Data Driven Analysis for Electricity Theft Attack-Resilient Power Grid," *IEEE Transactions on Power Systems*, vol. 38, no. 1, pp. 537–548, Jan. 2023, doi: 10.1109/TPWRS.2022.3162391.

[12] A. Kori, P. Sumalatha, A. P. Anantpuramu, and A. Pradesh, "Deep Neural Network-Based Electricity Theft Detection in Smart Grids," 2023. [Online]. Available: www.ijcrt.org

[13] Y. Bai, H. Sun, L. Zhang, and H. Wu, "Hybrid CNN-Transformer Network for Electricity Theft Detection in Smart Grids," *Sensors (Basel)*, vol. 23, no. 20, Oct. 2023, doi: 10.3390/s23208405.

[14] H. Iftikhar *et al.*, "Electricity theft detection in smart grid using machine learning," *Front Energy Res*, vol. 12, 2024, doi: 10.3389/fenrg.2024.1383090.

[15] I. Petrlik *et al.*, "Electricity Theft Detection using Machine Learning." [Online]. Available: www.ijacsa.thesai.org

[16] P. M. Kgaphola, S. M. Marebane, and R. T. Hans, "Electricity Theft Detection and Prevention Using Technology-Based Models: A Systematic Literature Review," *Electricity*, vol. 5, no. 2, pp. 334–350, Jun. 2024, doi: 10.3390/electricity5020017.

[17] A. Ullah, N. Javaid, M. Asif, M. U. Javed, and A. S. Yahaya, “AlexNet, AdaBoost and Artificial Bee Colony Based Hybrid Model for Electricity Theft Detection in Smart Grids,” *IEEE Access*, vol. 10, pp. 18681–18694, 2022, doi: 10.1109/ACCESS.2022.3150016.

[18] M. F. Guato Burgos, J. Morato, and F. P. Vizcaino Imacaña, “A Review of Smart Grid Anomaly Detection Approaches Pertaining to Artificial Intelligence,” Feb. 01, 2024, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/app14031194.

[19] Y. Sun, X. Sun, T. Hu, and L. Zhu, “Smart Grid Theft Detection Based on Hybrid Multi-Time Scale Neural Network,” *Applied Sciences (Switzerland)*, vol. 13, no. 9, May 2023, doi: 10.3390/app13095710.

[20] G. Lin *et al.*, “Electricity Theft Detection in Power Consumption Data Based on Adaptive Tuning Recurrent Neural Network,” *Front Energy Res*, vol. 9, Nov. 2021, doi: 10.3389/fenrg.2021.773805.

[21] M. Žarković and G. Dobrić, “Artificial Intelligence for Energy Theft Detection in Distribution Networks,” *Energies (Basel)*, vol. 17, no. 7, Apr. 2024, doi: 10.3390/en17071580.