International Journal of Scientific and Cognitive Innovation (www.ijsci.org)
|| Volume 2, Issue 7, July 2026 || Impact Factor: 3.5 |

Deep Learning Techniques for Smart Meter Electricity Theft Detection: A Review

[1]Abhijeet Kumar, [2]Mr. Balram Yadav
[1]*M.Tech Scholar, School of Electrical and Electronics Engineering, SCOPE Global Skills University, Bhopal, India,*
[2]*Associate Professor & HOD, School of Electrical and Electronics Engineering, SCOPE Global Skills University, Bhopal, India*

***Abstract*— Electricity theft is a major challenge for modern smart grids and Advanced Metering Infrastructure (AMI), as unauthorized consumption, meter tampering, abnormal load patterns, and fraudulent energy usage can cause significant technical and economic losses to power utilities. The large volume of data generated by smart meters provides an opportunity to identify abnormal electricity consumption patterns using advanced data-driven techniques. This review paper presents a comprehensive analysis of deep learning techniques used for smart meter electricity theft detection, with particular emphasis on LSTM, BiLSTM, GRU, hybrid deep learning, ensemble learning, and adaptive learning frameworks. The reviewed studies are analyzed with respect to detection accuracy, feature selection, data balancing, privacy preservation, false-positive reduction, synthetic theft generation, and the use of AMI-based electricity consumption data. The review also examines the role of benchmarking datasets and preprocessing techniques in improving the reliability of theft detection models. Furthermore, the study identifies major challenges including imbalanced theft data, evolving theft patterns, privacy concerns, false alarms, and generalization across different smart-grid environments. Overall, the review indicates that deep learning and hybrid intelligent techniques provide a promising foundation for developing reliable, adaptive, and scalable electricity theft detection systems for modern smart grids.**

Keywords: Smart Meter, Electricity Theft, CNN, Deep Learning, Smart Grid.

I. INTRODUCTION

Electricity theft is one of the major challenges faced by modern electrical power utilities because unauthorized electricity consumption can cause financial losses, inaccurate energy accounting, increased distribution losses, and difficulties in maintaining reliable power-system operation. The rapid deployment of Advanced Metering Infrastructure (AMI) and smart meters has changed the way electricity consumption is measured and monitored. Smart meters continuously record detailed electricity consumption information, making it possible to analyze consumer load profiles and identify unusual consumption behavior. In this environment, electricity theft detection has become an important research area for improving the security, efficiency, and economic performance of modern smart-grid systems [1].

Electricity theft generally involves unauthorized or fraudulent modification of electricity consumption behavior to reduce the amount of energy recorded by the meter. Such activities may include meter tampering, bypassing the meter, illegal connections, manipulation of measurement systems, or abnormal changes in consumption patterns. From an electrical-system perspective, these activities create discrepancies between the actual electricity supplied and the energy recorded by the metering infrastructure. The resulting losses can affect distribution-system planning, energy accounting, and utility revenue. Therefore, reliable identification of abnormal electricity consumption patterns is essential for maintaining accurate electrical energy measurement and efficient distribution-system operation [2].

The introduction of smart meters has provided utilities with high-resolution electricity consumption data that can be used for automated theft detection. Unlike conventional electricity meters, smart meters can record consumption at regular time intervals and communicate the measurements to utility systems. These time-series measurements provide information about variations in active power and energy consumption under normal operating conditions. When the recorded load profile deviates significantly from expected consumption behavior, it may indicate a potential abnormal or fraudulent condition. However, distinguishing genuine changes in consumer demand from actual electricity theft remains challenging because residential and commercial loads naturally exhibit considerable temporal variations [3].

The complexity of electricity consumption patterns makes electricity theft detection a challenging electrical data-analysis problem. Consumer demand can change according to time of day, weather conditions, occupancy, appliance operation, industrial activity, and seasonal variations. A sudden reduction in electricity consumption, for example, may be caused by legitimate reasons such as reduced occupancy or changes in appliance usage rather than theft. Similarly, electricity theft may be performed in ways that produce consumption patterns that appear similar to normal load behavior. Therefore, an effective detection system must be capable of identifying subtle abnormalities within historical electrical consumption profiles while minimizing incorrect identification of legitimate consumers [4].

Conventional electricity theft detection methods have traditionally relied on meter inspection, rule-based approaches, statistical analysis, and comparison of measured consumption with expected energy usage. Physical inspection can provide reliable evidence of meter tampering but requires considerable manpower, time, and operational cost. Rule-based techniques can identify predefined abnormal conditions but may have limited capability when theft patterns change or become more sophisticated. Statistical approaches can identify deviations from expected load behavior, but their performance may decrease when electricity consumption is highly nonlinear and variable. These limitations have encouraged the development of intelligent data-driven approaches capable of learning complex electricity consumption patterns automatically [5].

Machine learning techniques have provided an important advancement in automated electricity theft detection. Classification-based models can be trained using historical smart-meter data containing normal and fraudulent electricity consumption patterns. The models can learn relationships between electrical consumption characteristics and theft conditions and subsequently classify new observations. However, electricity consumption is inherently sequential, and the relationship between current consumption and previous measurements can provide important information for detecting abnormal behavior. Consequently, models that can learn temporal dependencies are particularly valuable for smart-meter electricity theft detection. This has encouraged the increasing application of deep learning techniques to AMI-based electricity consumption data [6].

Deep learning models can automatically learn hierarchical and nonlinear representations from large-scale smart-meter datasets. Recurrent architectures such as Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) are particularly suitable for electricity theft detection because they can learn temporal relationships within sequential consumption measurements. Electricity theft may not always be identifiable from a single meter reading; instead, a sequence of unusual consumption values may provide stronger evidence of abnormal behavior. LSTM and GRU models can therefore analyze historical consumption sequences and identify temporal characteristics associated with normal and fraudulent electricity usage. These capabilities make deep learning a promising approach for automated electricity theft detection in modern smart-grid environments [7].

Bidirectional and hybrid deep learning architectures provide further opportunities for improving electricity theft detection performance. BiLSTM models can process sequential information in both temporal directions within the available input sequence, while hybrid frameworks can combine feature extraction, classification, and optimization techniques. Such approaches are particularly useful when smart-meter datasets contain complex and nonlinear consumption patterns. Feature selection can also remove irrelevant electrical variables and reduce unnecessary model complexity, while data-balancing techniques can address the imbalance between normal electricity consumption and relatively fewer theft cases. Therefore, the integration of preprocessing, feature selection, balancing, and deep learning can provide a more comprehensive approach to electricity theft detection [8].

Despite significant developments, several challenges continue to affect the practical implementation of deep learning-based electricity theft detection systems. One major challenge is the class imbalance problem, as legitimate electricity consumption records generally far outnumber theft cases. Insufficient representation of theft patterns can cause models to favor the normal class and fail to identify actual theft events. Another important issue is the false-positive rate, because incorrectly classifying legitimate consumers as electricity thieves can result in unnecessary inspections and operational costs. Privacy is also an important consideration because detailed smart-meter data can reveal information about consumer activities and electricity usage behavior. Therefore, detection systems must achieve a suitable balance between detection accuracy, false-positive reduction, data privacy, and computational efficiency [9].

Considering these challenges, deep learning-based electricity theft detection has become an important research direction for improving the reliability and security of smart-grid metering systems. Recent studies have investigated adaptive deep learning, hybrid machine learning and deep learning, LSTM, GRU, BiLSTM, ensemble learning, feature selection, data balancing, privacy-preserving detection, and evolutionary optimization for identifying fraudulent electricity consumption. These developments indicate that intelligent models can provide more automated and scalable alternatives to conventional inspection-based approaches. However, further research is required to develop models that can accurately identify evolving theft patterns while maintaining low false-positive rates and protecting smart-meter data. Therefore, this study reviews major deep learning techniques for smart meter electricity theft detection, with emphasis on their detection capabilities, data requirements, temporal learning mechanisms, preprocessing strategies, limitations, and applicability to modern smart-grid electrical systems [10].

II. LITERATURE SURVEY

Chen et al. [1] presented LoadGuard, an adaptive deep learning model for electricity theft detection using smart-meter data. The study focused on identifying abnormal electricity consumption patterns associated with fraudulent usage in modern power systems. The adaptive learning capability of the model is particularly relevant because electricity theft patterns can change over time. The work demonstrates the potential of deep learning for improving the reliability of smart-meter-based electricity theft detection.

Lin et al. [2] developed a hybrid machine learning and deep learning framework for effective electricity theft detection in smart grids. The study combined different learning approaches to improve the identification of fraudulent electricity consumption patterns. Such hybridization can exploit the strengths of conventional machine learning and deep learning techniques for smart-grid data analysis. The work highlights the importance of integrated intelligent approaches for improving electricity theft detection performance.

Chen et al. [3] presented a hybrid deep learning model, termed Smart Energy Guardian, for detecting fraudulent photovoltaic (PV) generation. The study addressed fraudulent behavior associated with distributed PV energy generation, which is becoming increasingly important with the expansion of renewable-energy-based smart grids. The approach demonstrates how deep learning can be applied to identify abnormal generation patterns rather than focusing only on conventional household electricity theft. The study therefore extends intelligent energy-fraud detection toward modern distributed renewable-energy systems.

An et al. [4] investigated selective virtual synthetic vector embedding for full-range current harmonic suppression in a DC collector. Although the study primarily focuses on power-electronic control and harmonic suppression rather than electricity theft detection, it provides relevant insight into electrical signal characteristics and power-quality behavior. Such electrical measurements can potentially contribute to abnormal-condition identification in advanced electrical networks. The work emphasizes the importance of accurate electrical signal analysis in modern power systems.

Wu et al. [5] presented P2Detect, an electricity theft detection approach designed with privacy preservation for both data and models in smart grids. The study addressed an important challenge in smart-meter-based theft detection because electricity consumption data can contain sensitive information about consumer behavior. By incorporating privacy-preserving mechanisms, the approach attempts to maintain detection capability while protecting electricity-consumption information. The study highlights the importance of balancing theft detection performance with data and model privacy in smart-grid applications.

Zidi et al. [6] developed a theft detection dataset for benchmarking and machine-learning-based classification in a smart-grid environment. The study emphasized the importance of suitable datasets for developing and objectively evaluating electricity theft detection techniques. A representative dataset containing normal and fraudulent consumption patterns is essential for training and testing intelligent detection models. The work provides an important foundation for comparative evaluation of machine learning and deep learning approaches for electricity theft identification.

Pamir et al. [7] investigated synthetic theft attacks and LSTM-based preprocessing for electricity theft detection using a GRU model. The study focused on generating representative theft scenarios and using sequential deep learning techniques to identify fraudulent electricity consumption. The combination of LSTM-based preprocessing and GRU enables the model to capture temporal characteristics within smart-meter load profiles. The work demonstrates the importance of both realistic theft-data generation and temporal feature learning for improving electricity theft detection.

An et al. [8] investigated asymmetric topology design and quasi-zero-loss switching composite modulation for an IGCT-based high-capacity DC transformer. The primary focus of this study is power-electronic converter design rather than electricity theft detection. However, the work contributes to the broader field of modern electrical power systems by addressing efficient power conversion and switching operation. Such developments are relevant to smart-grid infrastructure because reliable power-electronic interfaces form an important component of advanced electrical networks.

Pamir et al. [9] presented an electricity theft detection framework using RFE-based feature selection and KNNOR-based data balancing, followed by a BiLSTM-Logit Boost stacking ensemble model. The study addressed two important problems in theft detection: irrelevant features and imbalanced normal-to-theft data distributions. The BiLSTM component enables the model to learn temporal relationships within electricity consumption sequences, while the ensemble strategy improves classification capability. The work demonstrates the effectiveness of combining feature selection, data balancing, and deep learning for smart-meter electricity theft detection.

Gu et al. [10] developed an electricity theft detection method for AMI using deep learning and an evolutionary algorithm, with particular emphasis on achieving a low false-positive rate. Reducing false positives is critical because incorrectly identifying legitimate consumers as electricity thieves can lead to unnecessary investigations and operational costs for utilities. The integration of deep learning with evolutionary optimization provides a mechanism for improving the detection process. The study highlights the importance of reliable and accurate theft identification for practical AMI-based smart-grid applications.

III. CHALLENGES

Deep Deep learning-based smart meter electricity theft detection faces several challenges because fraudulent electricity consumption can closely resemble legitimate variations in residential and commercial load patterns. Smart-meter data are generally large, time-dependent, and often highly imbalanced, while actual theft cases may represent only a small portion of the available observations.

International Journal of Scientific and Cognitive Innovation (www.ijsci.org)
|| Volume 2, Issue 7, July 2026 || Impact Factor: 3.5 |

In addition, changing consumer behavior, different types of theft, data privacy requirements, false alarms, and computational requirements can affect the reliability of detection systems. The major challenges are discussed below.

1. Imbalanced Electricity Theft Data

One of the major challenges is the imbalance between normal and fraudulent electricity consumption records. In practical smart-grid datasets, legitimate electricity consumption is usually much larger than confirmed theft cases. As a result, a deep learning model may become biased toward the normal class and fail to correctly identify relatively rare theft events. Appropriate data-balancing and synthetic-data-generation techniques are therefore required.

2. Complex and Changing Theft Patterns

Electricity theft does not always produce a fixed or easily recognizable consumption pattern. Different consumers may adopt different methods of unauthorized consumption, and theft behavior may change over time. Some fraudulent load profiles may appear similar to legitimate variations in electricity demand. Therefore, detection models must learn complex temporal characteristics rather than depending only on predefined rules.

3. High False-Positive Rate

Incorrectly identifying a legitimate consumer as an electricity thief is a serious practical problem for power utilities. A high false-positive rate can result in unnecessary field inspections, increased operational costs, and inconvenience to genuine consumers. Therefore, an effective deep learning model must not only detect theft accurately but also distinguish abnormal consumption from legitimate changes in electrical load.

4. Smart-Meter Data Quality

Smart-meter measurements may contain missing values, communication errors, measurement noise, abnormal readings, or inconsistent data intervals. Poor-quality electrical consumption data can negatively affect the training and testing of deep learning models. Data preprocessing, missing-value treatment, normalization, and outlier handling are consequently important for developing reliable theft detection systems.

5. Consumer Behavior Variations

Electricity consumption varies considerably between consumers because of differences in occupancy, appliance ownership, working schedules, lifestyle, and energy-use habits. A consumption pattern that appears abnormal for one household may be completely normal for another. This variation makes it difficult to develop a generalized theft detection model that performs consistently across different consumers and geographical regions.

6. Privacy and Security of Smart-Meter Data

Smart meters collect detailed information about electricity consumption, which may indirectly reveal household activities and usage behavior. Using such data for deep learning-based theft detection creates important privacy and security concerns. The detection framework must therefore provide effective theft identification while ensuring that sensitive consumer electricity information is appropriately protected.

7. High Computational Requirement

Deep learning architectures such as LSTM, GRU, BiLSTM, CNN, and hybrid ensemble models may require significant computational resources for training, particularly when high-resolution smart-meter datasets contain millions of time-series observations. Large models can also increase training time and memory requirements. Developing computationally efficient architectures is therefore important for practical deployment in utility-level monitoring systems.

8. Generalization and Real-Time Detection

A model trained using electricity consumption data from one utility, region, or group of consumers may not perform equally well in another environment. Changes in tariff structures, consumer behavior, electrical infrastructure, and theft techniques can affect model performance. Furthermore, practical smart-grid applications require rapid identification of suspicious consumption patterns. Therefore, future systems need to be adaptive, scalable, and capable of providing reliable real-time or near-real-time electricity theft detection.

IV. CONCLUSION

Deep learning techniques have emerged as effective approaches for detecting electricity theft from smart-meter and AMI-based electricity consumption data. The reviewed studies demonstrate that models such as LSTM, GRU, BiLSTM, hybrid deep learning, and ensemble frameworks can learn complex temporal and nonlinear patterns associated with normal and fraudulent electricity consumption. Advanced preprocessing, feature selection, data balancing, synthetic theft generation, and optimization techniques can further improve detection performance and reduce false-positive cases. However, challenges related to highly imbalanced datasets, changing theft patterns, data quality, consumer privacy, computational requirements, and model generalization continue to affect practical deployment. Overall, deep learning-based electricity theft detection provides a promising solution for improving energy accounting, reducing non-technical losses, and strengthening the reliability and security of modern smart-grid systems, while future research should focus on adaptive, privacy-preserving, computationally efficient, and real-time detection frameworks.

REFERENCES

[1] X. Chen, C. Huang, Y. Zhang and H. Wang, "LoadGuard: An Adaptive Deep Learning Model for Smart Meter Electricity Theft Detection," 2025 IEEE 23rd International Conference on Industrial Informatics (INDIN), Kunming, China, 2025, pp. 1-6, doi: 10.1109/INDIN64977.2025.11279201.

[2] H. Lin, G. Zhang and Z. Sun, "A Hybrid Machine Learning and Deep Learning Framework for Effective Electricity Theft Detection in Smart Grids," 2025 5th Asia-Pacific Conference on Communications Technology and Computer Science (ACCTCS), Shenyang, China, 2025, pp. 589-595, doi: 10.1109/ACCTCS66275.2025.00108.

[3] X. Chen, C. Huang, Y. Zhang, and H. Wang, “Smart energy guardian: A hybrid deep learning model for detecting fraudulent pv generation,” in 2024 IEEE International Smart Cities Conference (ISC2), 2024, pp. 1–6.

[4] F. An, B. Zhao, B. Cui, Y. Chen, L. Qu, Z. Yu, R. Zeng, “Selective Virtual Synthetic Vector Embedding for Full-Range Current Harmonic Suppression of the DC Collector,” IEEE Trans. Power Electronics., vol. 38, no. 2, pp. 2577–2588, Feb., 2023.

[5] Wu, H. Shi, S. Fu, Y. Luo, and M. Xu, “p2detect: Electricity theft detection with privacy preservation for both data and model in smart grid,” IEEE Transactions on Smart Grid, vol. 14, no. 3, pp. 2301–2312, 2023.

[6] S. Zidi, A. Mihoub, S. Mian Qaisar, M. Krichen, and Q. Abu Al-Haija, “Theft detection dataset for benchmarking and machine learning based classification in a smart grid environment,” Journal of King Saud University - Computer and Information Sciences, vol. 35, no. 1, pp. 13–25, 2023.

[7] Pamir, N. Javaid, S. Javaid, M. Asif, M. U. Javed, A. S. Yahaya, and S. Aslam, “Synthetic theft attacks and long short term memory-based preprocessing for electricity theft detection using gated recurrent unit,” Energies, vol. 15, no. 8, 2022, p. 2778.

[8] An, F., Zhao, B., Cui, B., Ma, Y., Zhang, X., Tang, X., & Dong, L. (2022). Asymmetric Topology Design and Quasi-Zero-Loss Switching Composite Modulation for IGCT-Based High-Capacity DC Transformer. IEEE Transactions on Power Electronics, 38(4), 4745–4759.

[9] Pamir, N. Javaid, A. Almogren, M. Adil, M. U. Javed, and M. Zuair, “RFE based feature selection and KNNOR based data balancing for electricity theft detection using BiLSTM-Logit Boost stacking ensemble model,” IEEE Access, vol. 10, 2022, pp. 112948–112963.

[10] D. Gu, Y. Gao, K. Chen, J. Shi, Y. Li, and Y. Cao, “Electricity theft detection in AMI with low false positive rate based on deep learning and evolutionary algorithm,” IEEE Transactions on Power Systems, vol. 37, no. 6, 2022, pp. 4568–4578.