© MAY 2026 | IRE Journals | Volume 9 Issue 11 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I11-1717927

Energy Theft Detection in Smart Grids Using Machine Learning: A Structured Review and Proposed Hybrid Framework

SHAIK HEERA[1], DR. HARIPRIYA V[2]
[1]*Dept. of Computer Science and Information Technology Jain (Deemed-to-be University), Jayanagar 9th Block Campus, Bengaluru, India*
[2]*Assistant Professor, Dept. Of Computer Science & IT, Jain University, Bangalore*

Abstract- ***Electricity theft is a critical challenge for global power utilities, causing annual losses estimated at USD 96 billion through meter tampering, illegal connections, and cyber manipulation of smart meter data. Traditional rule-based and manual inspection methods are inadequate against increasingly sophisticated theft techniques in modern smart grid environments. This paper presents a structured review of 25 IEEE-indexed publications (2022–2025) on machine learning-based energy theft detection, analysing methodologies, datasets, model architectures, and key limitations. Thematic classification identifies six major research directions: supervised classification, deep learning, hybrid and ensemble methods, IoT-integrated systems, anomaly detection, and satellite and geospatial AI approaches. Systematic gap analysis reveals ten critical deficiencies — including absence of real-time deployment, scalability constraints, limited temporal modelling, lack of automated alerts, and dataset imbalance — and maps fifteen targeted research questions and objectives. A novel intelligent hybrid ML-based energy theft detection framework is proposed, aimed at improving detection accuracy, enabling real-time automated alerting, and minimising electricity losses in smart grid environments.***

Keywords— Energy Theft Detection, Non-Technical Losses, Smart Grid, Machine Learning, Deep Learning, LSTM, Anomaly Detection, SVM, Ensemble Learning, IoT, Smart Meter, SMOTE.

I. INTRODUCTION

A. Background of the Study

Electricity theft, also known as non-technical loss (NTL), costs the global power industry an estimated USD 96 billion annually [1]. Theft methods range from direct meter tampering and illegal connections to sophisticated cyber manipulation of smart meter data, making detection increasingly complex in the era of smart grids. Traditional rule-based and manual inspection systems are reactive, labour labour-intensive, and incapable of keeping pace with evolving theft techniques.

The widespread deployment of smart meters and Advanced Metering Infrastructure (AMI) has created an unprecedented volume of granular, time-stamped consumption data. This richness enables machine learning (ML) models to learn the behavioural signatures of legitimate consumers and flag deviations consistent with theft — in real time and at scale [6][8].

B. Problem Statement

Despite significant research progress in ML-based energy theft detection, key gaps remain: most systems are validated offline on historical data, scalability to large networks is unproven, and automated alert mechanisms are largely absent. Traditional rule-based systems cannot adapt to new and evolving theft techniques. There is therefore a pressing need for an intelligent, scalable, real-time ML framework that integrates advanced feature engineering, hybrid modelling, and automated alerting for smart grid deployment.

C. Motivation

The motivation of this work arises from the consistent gap observed across all reviewed publications: high offline detection accuracy paired with critical deployment deficiencies. Classical classifiers such as Random Forest achieve over 95% accuracy but degrade at scale. Hybrid ML-DL models achieve the highest performance but require large labeled datasets and high compute. No existing

system combines scalable real-time inference with automated alert generation — a gap this framework is designed to address.

D. Objectives of the Study

The objectives of this research are:

- Analyse electricity consumption patterns using smart meter time-series data.
- Develop a supervised ML model for energy theft binary classification.
- Detect anomalies using unsupervised and semi-supervised methods.
- Improve detection accuracy through advanced feature engineering (statistical, temporal, wavelet).
- Handle imbalanced datasets using SMOTE and resampling techniques.
- Implement LSTM-based long-term time-series analysis for temporal theft pattern detection.

E. Contributions of the Paper

The main contributions of this work are:A structured comparative review of 25 IEEE publications (2022–2025) on ML-based energy theft detection.Identification of ten primary research gaps in existing energy theft detection systems.Fifteen targeted research questions and objectives mapped to the identified gaps.A proposed end-to-end intelligent hybrid ML-DL detection framework with real-time IoT integration and automated alerting.

II. LITERATURE REVIEW

A. Supervised Classification Models

Supervised classification is the most widely adopted category. Naveen Kumar et al. [3] achieved Accuracy=94.2% and F1=93.1% using Decision Tree, Random Forest, SVM, and KNN on smart meter data. Ahammad and Farid [21] and Lavanya et al. [24] both confirmed Random Forest as the strongest classical classifier, achieving over 95% and 94% accuracy respectively. Karthik V. et al. [25] replicated this finding with Random Forest consistently outperforming SVM, Logistic Regression, and Decision Tree. Sahoo et al. [7] further validated consumption pattern analysis as an effective feature strategy. Collectively, these studies establish Random Forest as the default supervised baseline for energy theft classification.

B. Deep Learning Approaches

Deep learning addresses the nonlinear temporal nature of theft patterns. Lakshmi and Gopal [2] deployed a DNN and GRU model integrated with IoT sensors, achieving 92.5% real-time detection accuracy — one of the few studies combining hardware and deep learning. Ness [17] developed a hybrid KNN-LSTM architecture on the SGCC dataset (2014–2016), achieving 81.32% accuracy. Malkar et al. [23] introduced the highest-performing model: a multiscale LSSVR-RELM-MHA-BiGRU model optimised with the Dung Beetle Optimizer (DBO), achieving 99.06% accuracy and AUC=0.9999 on the SGCC dataset. Subburaj et al. [20] proposed a hybrid NTM-LSTM model achieving 98.5% accuracy and F1=97.0%, demonstrating that memory-augmented deep networks significantly outperform standard LSTMs for long-term pattern detection.

C. Hybrid and Ensemble Methods

Hybrid models combine the interpretability of classical ML with the expressiveness of deep learning. Khan et al. [8] proposed a stacked ML and DL framework demonstrating that hybrid architectures outperform both standalone ML and standalone DL models. Lin et al. [12] developed an RF-SVM-Neural Network hybrid, confirming improved reliability across varied consumption profiles. Altamimi et al. [11] introduced time-series segmentation combined with ensemble classifiers (RF, Gradient Boosting), finding that temporal segmentation significantly enhances detection capability. Abbas et al. [6] introduced an active learning framework that significantly reduces labeling cost — a critical practical constraint in real-world grid deployments.

D. IoT-Integrated Systems

IoT-based systems bridge the gap between data collection and real-time detection. Akhil et al. [13] developed a low-cost IoT smart meter prototype achieving real-time theft detection with automated alerts. Karthik R.S. et al. [14] reported over 95% accuracy combining IoT sensors with Decision Tree, RF, and Naive Bayes classifiers. Thinakaran et al.

© MAY 2026 | IRE Journals | Volume 9 Issue 11 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I11-1717927

[22] achieved 99.2% detection accuracy and sub-second response time using ESP32-based threshold detection — the fastest response in the reviewed set. Abilesh et al. [5] proposed an integrated LSTM forecasting and SVM theft detection pipeline on a cloud platform, demonstrating that combining demand prediction with anomaly classification improves early theft identification.

E. Anomaly Detection and Data Challenges

Unsupervised and semi-supervised anomaly detection methods handle unlabeled data more practically. Venkatakrishnan et al. [4] applied K-Means, DBSCAN, Isolation Forest, and LOF with PCA dimensionality reduction, achieving high anomaly precision with minimal false positives. Amadhila et al. [10] applied K-Means and Isolation Forest on utility data from informal settlements (Silhouette ≈0.71). Qi et al. [19] introduced time-wavelet feature engineering with ensemble semi-supervised outlier detection, achieving AUC=0.9023 across 11 FDI attack types without any labeled theft data.

F. Satellite and Geospatial AI

Kaminski et al. [15] used CNN-based building detection on satellite imagery matched against utility meter databases to identify unregistered buildings — a form of theft invisible to meter-based systems. Hasan et al. [16] extended this with a CNN and GIS mapping pipeline achieving high detection accuracy and large-scale coverage. Gonzales et al. [18] analysed how check meter placement and loss-based features affect theft detection in networks with rooftop PV and net metering, finding ANN and SVM most effective in infrastructure-aware configurations.

III. COMPARATIVE ANALYSIS OF EXISTING METHODS

Table I presents a comparative summary of all 25 reviewed papers. Key observations: (1) Random Forest is the most consistently accurate classical classifier (>94%); (2) Hybrid ML-DL models achieve the highest accuracy — up to 99.06% [23] and 98.5% [20]; (3) IoT-integrated systems achieve fast response but often lack advanced ML; (4) No study has deployed a fully scalable, real-time automated theft detection and alert system; (5) Dataset imbalance, single-region training, and absence of labeled data are persistent challenges.

TABLE I Comparative Summary of All 25 Reviewed Papers

Ref	Authors (Year)	Method / Model	Performance
[1]	Kolade et al. (2023)	LR, RF, CNN, RNN, Autoencoders, GANs	ML >> traditional (review)
[2]	Lakshmi & Gopal (2024)	DNN + GRU + IoT sensors	92.5% acc.; real-time ETD
[3]	Naveen Kumar et al. (2022)	DT, RF, SVM, KNN	Acc=94.2%, F1=93.1%
[4]	Venkatakrishnan et al. (2025)	RF, K-Means, DBSCAN, Isolation Forest, LOF	High anomaly acc.; low FP
[5]	Abilesh et al. (2024)	LSTM (forecast) + SVM (detection)	High acc.; real-time ETD
[6]	Abbas et al. (2024)	RFAL, XGBoostAL, LGBMAL, CatBoostAL	RFAL: 70.61% acc.
[7]	Sahoo et al. (2023)	RF, DT, SVM	High acc.; RF best
[8]	Khan et al. (2022)	Stacked ML + Deep Neural Networks	Improved over conventional
[9]	Deepa K R et al. (2024)	Naive Bayes, DT, RF, SVM, J48, KNN	Naive Bayes ~100%; others >95%
[10]	Amadhila et al. (2024)	K-Means + Isolation Forest	Silhouette ≈0.71; effective ETD
[11]	Altamimi et al. (2024)	RF, Gradient Boosting, Ensemble	Ensemble >> single classifiers
[12]	Lin et al. (2025)	RF + SVM + Neural Network hybrid	Hybrid >> standalone ML
[13]	Akhil et al. (2023)	IoT sensors + ML classification	Real-time alerts; low cost
[14]	Karthik R.S. et al. (2024)	DT, RF, Naive Bayes + IoT	>95% acc.; real-time IoT
[15]	Kaminski et al.	CNN building	Improved

	(2024)	detection + GIS	unregistered bldg. detection
[16]	Hasan et al. (2024)	CNN + deep learning + GIS	High acc.; large-scale coverage
[17]	Ness (2025)	KNN + RF + XGBoost + LSTM (hybrid)	KNN+LSTM: 81.32% acc.
[18]	Gonzales et al. (2024)	SVM, ANN, DT + loss-based features	ANN & SVM highest w/ optimal meters
[19]	Qi et al. (2024)	PCA, ABOD, KNN, GMM, OCSVM, LOF, HBOS	Best AUC=0.9023 (EMAVG ensemble)
[20]	Subburaj et al. (2024)	NTM + LSTM hybrid	Acc=98.5%, F1=97.0%, RMSE=0.08
[21]	Ahammad & Farid (2024)	RF, SVM, Logistic Regression, KNN	RF >95% acc.
[22]	Thinakaran et al. (2024)	Threshold-based IoT anomaly detection	99.2% acc.; <1s response
[23]	Malkar et al. (2025)	LSSVR + RELM + MHA-BiGRU + DBO	99.06% acc.; AUC=0.9999
[24]	Lavanya et al. (2025)	RF, SVM, DT, KNN	RF: >94% acc.
[25]	Karthik V. et al. (2025)	RF, SVM, Logistic Regression, DT	RF: >95% acc.

IV. IDENTIFIED RESEARCH GAPS

Table II summarises ten primary research gaps derived from the 25-paper analysis. The most critical is the absence of real-time deployment validation — all reviewed systems were evaluated on offline historical datasets. The second critical gap is scalability: SVM and classical classifiers degrade with large smart grid data. The third is automated alert integration: even systems achieving >99% accuracy lack an end-to-end automated alert pipeline. The fourth is temporal modelling depth — LSTM-based studies limit sequences to short windows, missing multi-week theft patterns essential for detecting gradual tampering.

TABLE II Research Gaps and Proposed Contributions

Gap	Issue Identified	Proposed Contribution
G1 – Real-Time	Models validated offline only; no real-time deployment [1,6,7]	End-to-end real-time ML detection pipeline
G2 – Scalability	SVM and classical ML degrade on large-scale smart grid data [2,3]	Scalable framework tested on large datasets
G3 – Labeled Data	Deep learning requires expensive labeled theft samples [3,8]	Semi-supervised & active learning approaches
G4 – IoT Automation	IoT systems collect data but lack automated ML alert integration [4,13,14]	IoT + ML automated alert framework
G5 – Nonlinearity	Statistical/threshold methods miss complex theft patterns [10,22]	Advanced nonlinear ML anomaly detection
G6 – Alerts	Hybrid models evaluated in simulation; no live alert system [12,23]	Automated real-time alert mechanism
G7 – Integration	Forecasting and theft detection studied separately [5,7]	Unified demand forecasting + detection framework
G8 – Imbalance	SMOTE applied to single-region data only [8,19]	Multi-region imbalance-robust training strategy
G9 – Temporal	LSTM used for short sequences only; long-term patterns missed [11,17]	Long-term temporal theft pattern modeling
G10 – Adaptability	Rule-based systems cannot adapt to new or evolving theft types [6,22]	Adaptive intelligent ML detection system

V. PROPOSED METHODOLOGY

A. System Architecture

The proposed framework is a five-module end-to-end pipeline: (1) Smart Meter Data Ingestion — collects hourly and sub-hourly consumption readings from

AMI-enabled meters and IoT gateways; (2) Preprocessing and Feature Engineering — data cleaning, SMOTE-based class balancing, and feature extraction; (3) Model Training and Comparison — trains five model categories on an 80:10:10 time-series split; (4) Real-Time Detection Engine — runs inference on live data streams; (5) Automated Alert Module — generates utility notifications, flags suspect meters, and logs detections for audit purposes.

B. Feature Engineering

Features are drawn from four categories: (1) Statistical features — rolling mean, variance, skewness, kurtosis (24-hour and 7-day windows); (2) Temporal features — hour-of-day, day-of-week, holiday indicator, seasonal encoding; (3) Wavelet features — 3-level DWT coefficients (db1 basis) following Qi et al. [19]; (4) Deviation features — difference between LSTM-forecasted consumption and actual reading, enabling predictive anomaly identification as proposed by Abilesh et al. [5]. Feature selection via Mutual Information ranking reduces dimensionality while preserving discriminative power.

C. Dataset

The primary dataset is the State Grid Corporation of China (SGCC) smart meter dataset (2014–2016), widely used in the reviewed literature [17][23][19]. It contains daily electricity consumption records for approximately 42,372 consumers (3,565 labeled as theft) over 1,035 days. This dataset presents a realistic class imbalance (approximately 8.4% theft) that necessitates SMOTE-based oversampling. Additional evaluation will be conducted on utility datasets from informal settlements [10] to assess model generalisability across diverse grid environments.

D. Model Comparison Plan

Five model categories are benchmarked: (a) Baseline — Logistic Regression, Decision Tree; (b) Classical ML — RF, SVM, XGBoost, KNN; (c) Deep Learning — LSTM, Bi-LSTM, 1D-CNN; (d) Hybrid — KNN+LSTM [17], NTM+LSTM [20], RF+XGBoost+LSTM stacking; (e) Semi-supervised — Isolation Forest, Autoencoder, Ensemble SSOD [19]. Evaluation metrics: Accuracy, Precision, Recall, F1-Score, AUC-ROC, and False Positive Rate. Walk-forward cross-validation prevents data leakage in time-series splits.

E. Workflow

The implemented workflow consists of the following interconnected stages: (1) Historical smart meter consumption records are collected from the SGCC dataset; (2) Data preprocessing handles missing values, normalisation, and SMOTE-based class balancing; (3) Feature engineering extracts statistical, temporal, wavelet, and deviation features; (4) The dataset is divided into training (80%), validation (10%), and testing (10%) subsets chronologically; (5) All five model categories are trained and benchmarked; (6) The best-performing hybrid model is deployed in the real-time detection engine; (7) Automated alerts are generated for flagged meters.

G. Expected Outcomes

Target performance: Accuracy ≥97%, AUC-ROC ≥0.97, FPR ≤3%, real-time detection latency ≤30 seconds per reading cycle, and automated alert generation within 60 seconds. Benchmarked against best reported results: Malkar et al. [23] (99.06%, AUC=0.9999), Subburaj et al. [20] (98.5%, F1=97.0%), and Thinakaran et al. [22] (99.2% IoT detection). Occupancy-unaware and single-feature models are expected to underperform engineered hybrid approaches by 5–15% on F1-Score.

VI. CONCLUSION

This paper presents a structured review of 25 IEEE publications on ML-based energy theft detection, revealing a consistent pattern: high offline detection accuracy paired with critical deployment gaps — particularly the absence of real-time systems, scalability limitations, and missing automated alert mechanisms. Classical classifiers such as Random Forest achieve >95% accuracy reliably but degrade at scale. Hybrid ML-DL models (NTM-LSTM, KNN-LSTM, LSSVR-RELM-BiGRU) achieve the highest performance but require large labeled datasets and high compute.

The proposed intelligent framework addresses these gaps through end-to-end pipeline design combining advanced wavelet-based feature engineering, hybrid

model stacking, IoT-integrated real-time inference, and automated alerting. Future implementation work will focus on empirical benchmarking of all proposed models, live AMI system validation, and integration of privacy-preserving federated learning for consumer data protection.

VII. FUTURE SCOPE

Future implementation will focus on: (1) empirical benchmarking and comparative evaluation of all five model categories on the SGCC dataset; (2) live AMI system validation using real-time smart meter data streams; (3) multi-region dataset collection to improve model generalisability; (4) integration of privacy-preserving federated learning for consumer data protection in regulatory environments; (5) development of an end-to-end real-time automated alert system integrated with utility management platforms; and (6) exploration of explainable AI (XAI) techniques to improve model interpretability for utility operators.

REFERENCES

[1] A. O. Kolade, B. B. Adetokun, and O. Oghorada, "Energy Theft Detection in Power System Network: Reviews of Studies on Machine Learning Based Solutions," IEEE Conf. Paper, 2023.

[2] Lakshmi G and R. Gopal, "Design and Development of IoT Prototype for Real-Time Theft Detection and Optimization of Electricity Using Machine Learning Techniques," ICCDA, IEEE, 2024.

[3] S. N. Kumar, P. Rajesh, and K. S. Rao, "Machine Learning Based Electricity Theft Detection in Smart Grid Systems," IEEE Conf., 2022.

[4] G. R. Venkatakrishnan et al., "Anomaly Detection in Smart Metering: Clustering-Based Identification of Energy Theft," ICCCT, IEEE, 2025.

[5] Abilesh K. S. et al., "Revolutionizing Energy Management System with Machine Learning based Energy Demand Prediction and Theft Detection," ICACCS, IEEE, 2024.

[6] S. Abbas et al., "Improving Smart Grids Security: An Active Learning Approach for Smart Grid-Based Energy Theft Detection," IEEE Access, vol. 12, 2024.

[7] S. Sahoo, R. Mishra, and P. K. Rout, "Machine Learning Based Detection of Electricity Theft in Smart Grid Using Consumption Pattern Analysis," ICPEC, IEEE, 2023.

[8] I. U. Khan, N. Javeid, C. J. Taylor, K. A. A. Gamage, and X. Ma, "A Stacked Machine and Deep Learning-Based Approach for Analysing Electricity Theft in Smart Grids," IEEE Trans. Smart Grid, vol. 13, no. 2, 2022.

[9] Deepa K R et al., "Accuracy Enhance of Smart Energy Theft Detection Using Machine Learning Classifiers," ICITEICS, IEEE, 2024.

[10] M. N. Amadhila, A. K. Shikongo, and H. Tjombonde, "Electricity Theft Detection Machine-Learning Models for Windhoek Informal Settlements," IEEE Conf., 2024.

[11] E. Altamimi et al., "Improving Energy Theft Detection through Time Series Segmentation and Ensemble Learning," IECON, IEEE, 2024.

[12] H. Lin, G. Zhang, and Z. Sun, "A Hybrid Machine Learning and Deep Learning Framework for Effective Electricity Theft Detection in Smart Grids," ACCTCS, IEEE, 2025.

[13] K. H. Akhil et al., "Enhanced Low Cost Smart Energy Meter with Theft Detection using IoT," ICIMIA, IEEE, 2023.

[14] R. S. Karthik, P. Deepa, M. Keerthana, and S. Harini, "IoT Based Smart Energy Meter for Electricity Theft Detection and Monitoring," IEEE Conf. Proc., 2024.

[15] A. M. Kaminski et al., "Assignment of AI Detected Buildings from Satellite Images to Registered Meters for Energy Theft Detection," ISGT, IEEE, 2024.

[16] M. M. Hasan, S. Ahmed, M. R. Islam, and T. Rahman, "Assignment of AI Detected Buildings from Satellite Images to Registered

Meters for Energy Theft Detection," IEEE Conf. Proc., 2024.

[17] S. Ness, "Hybrid KNN-LSTM Framework for Electricity Theft Detection in Smart Grids Using SGCC Smart-Meter Data," IEEE Access, vol. 13, 2025.

[18] K. M. V. Gonzales et al., "Effect of Check Meter Quantity on Theft Detection in Distribution Networks with Rooftop PV and Net Metering," TENCON, IEEE, 2024.

[19] R. Qi, W. Japp, S. Pan, J. Zheng, and S. Shao, "Enhancing the Performance of Semi-supervised Electricity Theft Detection in Smart Grids with Feature Engineering and Ensemble Learning," KPEC, IEEE, 2024.

[20] T. Subburaj et al., "Enhancing Electricity Theft Detection and Loss Prediction in Metro Cities Using Hybrid Machine Learning Model," PDGC, IEEE, 2024.

[21] M. Ahammad and D. Md. Farid, "Detection of Electricity Theft Using Machine Learning Techniques," IEEE Conf. Proc., 2024.

[22] R. Thinakaran et al., "Smart Energy Management System Using IoT for Real-Time Monitoring and Theft Detection," ICITDA, IEEE, 2024.

[23] R. M. Malkar et al., "A Hybrid Deep Learning and Machine Learning Approach for Optimizing Electricity Theft Detection," ICICNCT, IEEE, 2025.

[24] D. Lavanya, P. R. Karthikeyan, S. Nithya, and R. Prabha, "Electricity Theft Detection Using Machine Learning Techniques," ICSSET, IEEE, 2025.

[25] V. Karthik, S. Deepa, M. Harish, and R. Santhosh, "Intelligent Electricity Theft Detection System Using Machine Learning Algorithms," ICACCS, IEEE, 2025.