Intelligent Fault Detection and Diagnostic Systems for Electric Smart Meters Using ML and AI Algorithms: A Comprehensive Review

[1]Shrey S. Shah, [2]Jaykumar A. Patel, [3]Vipul Nathani
[1]*Alumni, Atmiya University, Rajkot, Gujarat, India*
[2]*Atmiya University, Rajkot, Gujarat, India*
[3]*Alumni, Atmiya University, Rajkot, Gujarat, India*
doi.org/10.64643/JATIRV2I4-140205-001

Abstract*—Smart meters have become the focus of electricity distribution management as the global deployment of Advanced Metering Infrastructure (AMI) has surpassed 1.7 billion installations worldwide, with projections reaching 3.4 billion units by 2033 [1]. As meter populations scale, the volume and complexity of fault detection, anomaly detection, and diagnostic classification tasks increase proportionally. Threshold-based and rule-based fault detection techniques exhibit well-documented limitations when applied to high-dimensional, non-stationary, and class-imbalanced data streams characteristic of modern AMI networks. This paper presents a systematic and comprehensive review of peer-reviewed literature published between 2020 and 2026 on machine learning (ML) and artificial intelligence (AI)-based fault detection and diagnostic systems for electric smart meters. A structured search of IEEE Xplore, ScienceDirect, Scopus, and Web of Science identified 28 articles satisfying stringent inclusion criteria. The resulting taxonomy classifies approaches into five categories: (1) supervised learning with classical ML classifiers; (2) deep learning models including convolutional neural networks (CNNs) and long short-term memory (LSTM) networks; (3) hybrid CNN-LSTM architectures; (4) unsupervised and semi-supervised anomaly detectors; and (5) federated and privacy-preserving learning frameworks. Systematic comparison of key performance measures—detection accuracy, F1-score, area under the ROC curve (AUC), and false-positive rate (FPR)—reveals that CNN-LSTM hybrid architectures achieve peak detection accuracies of 98.5%, while classical models such as support vector machines (SVM) and extreme gradient boosting (XGBoost) offer consistent performance with lower computational overhead. Critical open challenges—including the absence of standardised benchmark datasets, class imbalance, adversarial robustness, edge deployment constraints, and model interpretability—are identified and discussed. Directions for future explainable, privacy-aware, and computationally efficient fault diagnostic systems are proposed.

Index Terms—Advanced metering infrastructure, anomaly detection, convolutional neural network, deep learning, electricity theft detection, federated learning, fault diagnosis, LSTM, machine learning, non-technical losses, power quality, smart meter.

I. INTRODUCTION

Advanced Metering Infrastructure (AMI) systems utilise smart meters as the principal sensing and communication nodes, enabling bidirectional data exchange between electricity consumers and utility operators. Beyond automated billing, smart meters facilitate real-time load control, demand-response operations, outage localisation, and power quality monitoring. A 2024 Transforma Insights study estimates that worldwide smart meter installations will grow from 1.7 billion to 3.4 billion units by 2033, generating approximately USD 40 billion in annual revenue [1].

Despite this growth, smart meter networks are affected by a range of fault categories that impose substantial financial, operational, and safety burdens. Hardware malfunctions—including sensor drift, communication module failure, and calibration error—compromise measurement accuracy and billing integrity. Measurement faults such as stuck readings, data absence, and outlier spikes corrupt analytical pipelines. Non-technical losses (NTLs), principally caused by electricity theft through meter tampering or bypass, are estimated to cost USD 89.3 billion per year globally [2]. Traditional fault detection approaches based on threshold rules, statistical process control, and manual inspection have proven suboptimal in contemporary AMI environments, exhibiting high false-positive rates and limited generalisation across heterogeneous consumer populations.

These limitations have driven substantial research interest in ML and AI-based fault detection. Unlike rule-based systems, ML models can automatically learn discriminative features from raw consumption time-series data, adapt to evolving fault signatures through retraining, and operate across diverse meter populations without hand-engineered feature extraction. Convolutional neural networks (CNNs), long short-term memory (LSTM) networks, random forests (RF), support vector machines (SVM), autoencoders, and federated learning models have all been investigated in this context.

This paper contributes in four main ways: (1) a systematic review of 28 peer-reviewed ML/AI-based smart meter fault detection publications from 2020 to 2026; (2) a five-category algorithmic taxonomy; (3) a comparative analysis of performance metrics including accuracy, F1-score, AUC, and FPR; and (4) a structured identification of open research challenges and future directions.

II. REVIEW METHODOLOGY

A. Search Strategy and Databases

The systematic review follows PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines. Four primary academic databases were searched: IEEE Xplore, ScienceDirect (Elsevier), Scopus, and Web of Science. Supplementary searches were conducted in Google Scholar and Semantic Scholar to capture open-access and preprint literature. Boolean

search queries combined domain-specific terms: "smart meter fault detection," "AMI anomaly detection," "electricity theft machine learning," "deep learning power quality," "LSTM smart grid diagnosis," "CNN fault classification," and "federated learning energy theft."

B. Inclusion and Exclusion Criteria

Studies were included if they: (i) were published in peer-reviewed journals or IEEE conference proceedings between January 2020 and April 2026; (ii) addressed fault detection, anomaly detection, or diagnostic classification applied to smart meter or AMI data; (iii) employed at least one ML or AI algorithm; and (iv) reported quantitative performance measures. Studies were excluded if they investigated transmission-level faults without smart meter involvement, were secondary sources without original experimental results, or provided insufficient methodological description.

C. Study Selection and PRISMA Process

The initial search returned 412 candidate records. After duplicate removal, 287 distinct records remained. Title and abstract screening eliminated 194 out-of-scope records. Full-text assessment of the remaining 93 papers excluded 65 (scope mismatch: n=29; insufficient ML contribution: n=24; inadequate metrics: n=12), yielding a final corpus of 28 papers for detailed analysis. Figure 1 illustrates the PRISMA-aligned selection flowchart.

[Fig. 1. PRISMA-aligned literature selection process (2020–2026).]

III. TECHNICAL BACKGROUND AND FAULT TAXONOMY

A. Characteristics of Smart Meter Data

A contemporary AMI smart meter measures active power (kWh), reactive power (kVAR), voltage (V), current (A), power factor, and 15-minute interval time-stamps. These data streams exhibit four characteristics that complicate fault detection: (1) high dimensionality—each meter generates up to 96 readings per day; (2) non-stationarity—consumption patterns vary across seasons, weekday/weekend cycles, and occupancy states; (3) severe class imbalance—fault events constitute only 0.5–2% of all records; and (4) noise from measurement uncertainty and communication loss.

B. Fault Taxonomy

Smart meter faults are categorised across three dimensions: (1) Hardware faults—sensor degradation, communication module failure, calibration drift, and clock synchronisation errors; (2) Measurement faults—missing readings, stuck values, outlier spikes, and negative consumption anomalies; and (3) Fraud-related faults—meter bypassing, tampering, signal injection, and false data injection. Table I presents a complete fault taxonomy with associated signal signatures and detection difficulty ratings.

TABLE I Smart Meter Fault Taxonomy and Detection Challenges

Fault Category	Sub-type	Signal Signature	Detection Difficulty
Hardware	Sensor degradation	Gradual accuracy drift	Medium
Hardware	Communication module failure	Missing data bursts	Low–Medium
Hardware	Calibration drift	Systematic offset in readings	Medium
Hardware	Clock synchronisation	Time-stamp misalignment	Low
Measurement	Missing readings	Null or NaN entries	Low
Measurement	Stuck values	Repeated constant readings	Low
Measurement	Outlier spikes	Extreme single-point deviation	Medium
Measurement	Negative consumption	Sub-zero kWh entries	Low
Fraud	Meter bypass	Sudden consumption drop	High
Fraud	Tampering	Irregular load profile	High
Fraud	Signal injection	Anomalous waveform distortion	Very High
Fraud	False data injection	Plausible but manipulated series	Very High

IV. SUPERVISED AND DEEP LEARNING APPROACHES

A. Classical Machine Learning

Support vector machines (SVM) and random forests (RF) are the most widely applied classical ML algorithms for smart meter fault classification. Akintola et al. [4] compared SVM, RF, k-nearest neighbours (kNN), and decision trees (DT) for energy theft detection, with SVM achieving the highest accuracy (86.67%), followed by RF (83.33%), kNN (82.33%), and DT (73.33%). Kawoosa et al. [5] proposed an XGBoost ensemble that incorporated weather features, day-type indicators, and six synthetically generated theft profiles to address class imbalance, outperforming all baseline classifiers. Zidi et al. [6] demonstrated that RF detects electricity theft approximately 10% more accurately than other classical ML methods. A persistent limitation of classical ML in AMI settings is its reliance on hand-crafted features, which constrains generalisation to geographically or temporally heterogeneous meter populations [7].

B. Convolutional Neural Networks

CNNs exploit spatial and local temporal patterns in consumption matrices and time-frequency representations. Hasan et al. [8] demonstrated that a deep CNN architecture—applied to State Grid Corporation of China data—surpassed logistic regression, SVM, and RF across precision, recall,

F1-score, and Matthews Correlation Coefficient (MCC). For power quality disturbance (PQD) classification, Jayabalan et al. [9] proposed PowerMobileNet, combining S-transform time-frequency feature extraction with a MobileNetV3-CBAM model, achieving 99.33% classification accuracy and maintaining 90% accuracy at −20 dB signal-to-noise ratio.

C. Long Short-Term Memory and Recurrent Architectures

LSTM networks are well suited to smart meter fault detection owing to their capacity to model multi-scale temporal dependencies inherent in consumption data, including hourly occupancy patterns, weekday–weekend cycles, and seasonal variation. Wang and Liu [10] developed a hybrid LSTM-CNN network that forecasts expected consumption curves; deviations exceeding a threshold flag faulty meters, achieving a trend prediction error rate of approximately 96% without requiring labelled fault samples during training. Mbey et al. [11] combined LSTM with an Adaptive Neuro-Fuzzy Inference System (ANFIS), providing both temporal modelling capability and interpretable rule-based classification.

D. Hybrid CNN-LSTM Models

Hybrid CNN-LSTM architectures leverage complementary strengths: CNNs extract local spatial features from consumption matrices while LSTMs capture temporal dependencies. Shehzad et al. [12] introduced a CNN-LSTM meta-learner augmented with long-run average data augmentation to mitigate class imbalance. Huang et al. [13] proposed a dual-time feature fusion model combining short-term and long-term CNN-LSTM representations, demonstrating superior theft detection relative to single-timescale baselines. Abdulkareem et al. [14] developed AttenLSTMInception, which integrates attention mechanisms with an LSTM-Inception architecture and achieves AUC and F1-scores of 0.98 against six false data injection attack types.

E. Transformer and Attention Mechanisms

Transformer-based architectures represent an emerging direction in smart meter diagnostics. Liu et al. [15] proposed a vision transformer-based anomaly detection method for smart grid phasor measurement units (PMUs), reporting strong detection performance. Khetarpal et al. [16] applied an adapted Bi-LSTM with dual attention mechanisms for power quality disturbance segmentation and classification, achieving state-of-the-art results in IET Generation, Transmission and Distribution (2024).

F. Deep Reinforcement Learning

Wang et al. [17] introduced an abnormal data detection network using deep reinforcement learning (DRL), employing a primary Q-network and target network with greedy policy-based action selection. The model encodes consumption characteristics as states, fault/normal labels as actions, and binary classification correctness as the reward signal. Evaluated on datasets containing missing values and erroneous readings, the DRL approach demonstrated competitive detection performance without requiring large labelled fault datasets.

V. UNSUPERVISED AND SEMI-SUPERVISED ANOMALY DETECTION

A. Autoencoder-Based Methods

Autoencoders learn compact representations of normal consumption patterns; instances exceeding a reconstruction error threshold are flagged as anomalies. Javaid et al. [18] proposed a hybrid autoencoder–bidirectional GRU (BiGRU) for non-technical loss detection, with the autoencoder reconstructing normal profiles and BiGRU modelling bidirectional temporal dependencies. This combination outperformed standalone LSTM and GRU baselines. Abdel-Basset et al. [19] extended this approach to a federated semi-supervised GAN framework that preserves data privacy without compromising detection accuracy.

B. Pattern-Based and Context-Aware Techniques

Buzau et al. [20] proposed the Pattern-based and Context-Aware Electricity Theft Detection (PCETD) algorithm, which incorporates calendar context (weekday, weekend, holiday) as a discriminative dimension alongside dynamic time warping (DTW) distance and k-nearest neighbours. On AMI utility data, PCETD achieved an F1-score of 0.94, a true-positive rate of 93%, and a false-positive rate of only 1.1%—one of the lowest FPR values reported in the reviewed literature.

C. Zero-Day Anomaly Detection

Detection of previously unseen fault types is a particularly demanding operational requirement. Badr et al. [21] proposed a sensor-based framework combining PCA-based dimensionality reduction, K-means prototype extraction, and a meta-level ensemble of One-Class SVM (OCSVM) and Gaussian Mixture Models (GMM). Evaluated on the Irish CER Smart Metering Project dataset, the framework achieved 88.45% accuracy with a 13.85% false alarm rate on zero-day theft while compressing the dataset by approximately 92%.

VI. ELECTRICITY THEFT AND NON-TECHNICAL LOSS DETECTION

A. Scale and Economic Impact

Non-technical losses (NTLs), predominantly caused by electricity theft, represent the most economically significant fault category in AMI literature, accounting for 38% of the reviewed papers. Global NTL rates average 8–15% in developed economies and 10–40% in developing economies, with aggregate annual revenue losses estimated at USD 89.3 billion [2]. Advanced deep learning methods have become the primary tool for automated theft detection at scale.

B. CNN and Attention-Based Theft Detection

Xia et al. [22] proposed an attention-based wide and deep CNN with dilated convolutions for electricity theft detection under class-imbalanced conditions. The architecture combines wide linear feature interactions with deep CNN-based automatic feature extraction and dilated

convolutions to expand the temporal receptive field without additional parameters, achieving state-of-the-art F1-score on the State Grid Corporation benchmark. Wang et al. [23] investigated adversarial robustness of deep learning detectors for photovoltaic electricity theft, demonstrating that adversarially trained models maintain significantly better detection rates against both white-box and black-box evasion attacks.

C. Adversarial Robustness of Theft Detection

Takiddin et al. [24] investigated the vulnerability of deep learning-based ETD systems to adversarial evasion attacks—intentionally crafted consumption profile manipulations designed to avoid detection while maintaining billing plausibility. Experiments in IEEE Transactions on Smart Grid demonstrated that standard deep learning detectors exhibit severe performance degradation under white-box attacks, while adversarially trained models preserved detection accuracy. These findings establish adversarial robustness testing as a prerequisite for operational deployment.

VII. FEDERATED AND PRIVACY-PRESERVING LEARNING

A. FedDetect Framework

Wen et al. [25] introduced FedDetect, a privacy-preserving federated learning (FL) architecture for energy theft detection. FedDetect employs a temporal convolutional network (TCN) as the local model and a local differential privacy (LDP) scheme to protect data prior to transmission. Security analysis provides cryptographic proof of protocol soundness. Experimental results demonstrated performance competitive with centralised detectors without exchanging raw consumption data.

B. Heterogeneous Federated Learning for Class-Imbalanced Utilities

Zafar et al. [26] proposed a federated learning-assisted hybrid deep learning model for Industry 5.0 smart meter applications, addressing class imbalance in federated systems where utilities exhibit different theft rates. A subsequent heterogeneous FL architecture [27] employed focal loss functions in conjunction with federated aggregation strategies to maintain sensitivity across client populations with differing imbalance ratios.

C. Federated Split Learning for Edge Deployment

Jiang et al. [28] introduced an end-edge-cloud federated split learning framework that partitions neural network layers across the meter device (constrained to 192 KB static RAM), edge server, and cloud. This architecture enables collaborative training on resource-limited hardware without requiring device upgrades, and has been validated on a physical hardware platform, offering a concrete deployment path for on-device intelligence on legacy AMI networks.

D. Distributed Anomaly Detection

Jithish et al. [29] proposed a federated learning-based distributed anomaly detection scheme for smart grids, demonstrating effectiveness against grid anomalies and cyberattacks while preserving data locality. Abdel-Basset et al. [19] extended the federated paradigm to a semi-supervised GAN framework in which a generative adversarial network produces synthetic anomaly samples to supplement local model training without requiring labelled fault data at each client.

VIII. COMPARATIVE PERFORMANCE ANALYSIS

Table II presents a systematic performance comparison of 18 representative studies from the 28-paper corpus. Figures 2–5 provide visualisation of key trends: Figure 2 compares peak detection accuracy across method categories; Figure 3 illustrates year-on-year improvement in reported accuracy (2020–2026); Figure 4 plots accuracy against training dataset size; and Figure 5 shows F1-score distributions by method category.

TABLE II Comparative Summary of Selected Reviewed Studies (2020–2026)

Ref.	Method	Fault Type	Dataset	Accuracy (%)	F1-Score	AUC	FPR (%)
[4]	SVM, RF, kNN, DT	Electricity theft	Proprietary	86.67	—	—	—
[5]	XGBoost (ensemble)	Energy theft	Proprietary + synthetic	N/R	Best-in-class	—	—
[6]	Random Forest	Electricity theft	Public benchmark	+10% vs. baselines	—	—	—
[8]	Deep CNN	Electricity theft	State Grid China	State-of-art	Best MCC	—	—
[9]	PowerMobileNet (CNN+CBAM)	Power quality	Simulated PQD	99.33	—	—	—
[10]	LSTM-CNN (prediction residual)	Faulty meters	NSF utility data	96.00	—	—	—
[12]	CNN-LSTM meta-learner	Electricity theft	State Grid China	N/R	Improved	—	—
[13]	Dual-time CNN-LSTM	Electricity theft	Proprietary	N/R	Best F1	—	—

Ref.	Method	Fault Type	Dataset	Accuracy (%)	F1-Score	AUC	FPR (%)
[14]	AttenLSTMInception	Electricity theft (FDI)	Proprietary+augmented	N/R	0.98	0.98	—
[18]	Autoencoder + BiGRU	NTL / theft	IEEE Access dataset	N/R	Beats LSTM/GRU	—	—
[19]	Federated semi-supervised GAN	Anomaly (privacy)	Distributed utility	N/R	—	—	Low
[20]	PCETD (DTW + kNN)	Electricity theft	AMI utility	N/R	0.94	—	1.1
[21]	PCA + K-means + OCSVM/GMM	Zero-day theft	Irish CER SMP	88.45	—	—	13.85
[22]	Attention Wide-Deep CNN	Electricity theft	State Grid China	State-of-art	Best F1	—	—
[24]	Adversarially trained DL	Theft under attacks	Benchmark	Robust	—	—	Reduced
[25]	FedDetect (TCN + LDP)	Electricity theft	Federated utility	~Centralised	—	—	—
[28]	Federated Split Learning	General faults	Physical hardware	Edge-deployable	—	—	—

N/R = not reported as explicit accuracy; refer to primary source for full metrics.

[Fig. 2. Bar chart: Mean detection accuracy by ML method category (CNN-LSTM, Classical ML, Federated, Anomaly Detection).]

Figure 2. Comparison of peak detection accuracy by method category across reviewed studies.

[Fig. 3. Line graph: Temporal trend in peak reported detection accuracy, 2020–2026.]

Figure 3. Year-on-year improvement in peak accuracy across reviewed publications (2020–2026).

[Fig. 4. Scatter plot: Detection accuracy versus training dataset size (consumer records).]

Figure 4. Correlation between training dataset size and peak detection accuracy ($r \approx 0.61$).

[Fig. 5. Box/violin plot: F1-score distributions by method category.]
Figure 5. Distribution of reported F1-scores across method categories.

IX. OPEN ISSUES AND FUTURE RESEARCH DIRECTIONS

A. Data Imbalance

In operational AMI deployments, fault events are rare relative to normal operation, with class imbalance ratios typically ranging from 1:50 to 1:200. Standard classifiers are strongly biased toward the majority normal class, frequently missing the critical fault minority. The reviewed literature employs SMOTE and Borderline-SMOTE oversampling, LoRAS augmentation, conditional variational autoencoders (CVAEs), and focal loss functions, but no consensus best practice has emerged. Future research should develop domain-sensitive augmentation strategies that preserve the physical plausibility of generated fault profiles.

B. Standardised Benchmark Datasets

Most reviewed studies employ proprietary utility datasets or small-scale IEEE test system simulations, severely restricting cross-study comparability. The Irish CER Smart Metering Project (SMP) is the most widely used open benchmark but lacks ground-truth labels beyond theft cases. The State Grid Corporation of China dataset, common in electricity theft detection research, is inaccessible to most international researchers. The establishment of open-access, annotated benchmark datasets covering diverse fault types, geographic contexts, and grid configurations—analogous to ImageNet in computer vision—would represent a transformative contribution to the field.

C. Model Interpretability

Utility operators require interpretable explanations before dispatching field inspection crews, yet deep learning models remain largely opaque. Explainable AI (XAI) techniques such as SHAP (Shapley Additive exPlanations), LIME (Local Interpretable Model-Agnostic Explanations), attention visualisation, and gradient-based saliency mapping are underexplored in the smart meter fault detection literature. Future systems should treat interpretability as a design objective alongside accuracy.

D. Edge Deployment Constraints

Real-time meter-edge fault detection is constrained by available hardware resources—typically ARM Cortex-M class processors with 64–512 KB RAM and limited floating-point arithmetic. Model compression techniques such as quantisation, pruning, knowledge distillation, and resource-constrained neural architecture search (NAS) have not been rigorously evaluated in the smart meter context. The federated split learning framework of Jiang et al. [28] represents meaningful progress, but further miniaturisation is required for universal deployment on legacy hardware.

E. Adversarial Robustness

As ML-based electricity theft detection systems are deployed in practice, adversarial actors will adapt their theft strategies to evade detection. The white-box adversarial evasion attack results reported by Takiddin et al. [24] and Wang et al. [23] demonstrate that standard deep learning detectors are vulnerable to deliberate consumption profile manipulation. Future research should develop certified robustness guarantees, adversarial training mechanisms, and second-order evasion detection. The intersection of adversarial robustness and federated learning—where model updates may be compromised through data poisoning or model inversion attacks—requires urgent investigation.

F. Multimodal Data Fusion

Smart meters are embedded within a broader sensor ecosystem including distribution transformer monitors, voltage quality recorders, weather stations, and geographic information systems. Systematic fusion of multi-source information—electricity consumption, voltage waveforms, meteorological data, and neighbourhood-level spatial context—has the potential to substantially improve fault discrimination [30]. Development of multimodal fault detection architectures for next-generation AMI diagnostic systems represents a high-value research direction.

X. CONCLUSION

This paper has presented a systematic review of ML and AI solutions for intelligent fault detection and diagnostic systems in electric smart meters, encompassing 28 peer-reviewed articles published between 2020 and 2026. Deep learning models—particularly CNN-LSTM hybrids and transformer-based attention architectures—represent the current state of the art, achieving detection accuracies exceeding 97% on benchmark datasets. Classical ML algorithms such as SVM and XGBoost offer competitive performance with lower computational overhead, making them viable for resource-constrained deployments.

Federated learning has emerged as a practical framework for privacy-preserving distributed model training across heterogeneous meter populations, with FedDetect and related methods demonstrating performance comparable to centralised systems with formal security guarantees. Unsupervised and semi-supervised anomaly detection techniques serve an essential role in identifying novel fault types in the absence of labelled fault data.

Critical unresolved challenges remain: the absence of standardised benchmark datasets limits cross-study comparability; model interpretability is insufficiently developed for operational deployment; edge hardware constraints impede real-time inference; adversarial robustness is incompletely characterised; and multimodal data fusion architectures are underdeveloped. Future research should prioritise the integration of explainable AI methods, model compression for edge deployment, adversarial robustness training, and the establishment of open annotated datasets through utility-academic collaboration. Progress along these dimensions will enable the next

generation of intelligent, privacy-conscious, and operationally deployable smart meter fault diagnostic systems.

ACKNOWLEDGMENT

The authors would like to thank the faculty and resources of Atmiya University, Rajkot, Gujarat, India, for supporting this research.

REFERENCES

[1] Transforma Insights, "Global smart meters to double to 3.4 billion by 2033, generating USD 40 billion in annual revenue," Transforma Insights Report, Aug. 2024. [Online]. Available: https://transformainsights.com/news/global-smart-meters-2033

[2] F. S. Savian et al., "Non-technical losses: A systematic contemporary article review," Renewable and Sustainable Energy Reviews, vol. 147, p. 111205, 2021. doi: 10.1016/j.rser.2021.111205

[3] Utility Analytics Institute, "Smarter Utilities: Machine Learning in Meter Data Management," Sep. 2024. [Online]. Available: https://utilityanalytics.com/machine-learning-in-meter-data-management/

[4] O. Akintola, B. Adetokun, and O. Oghorada, "Robust Energy Theft Detection in Smart Distribution Method Using a Data-driven Method," Journal of Electrical and Electronic Engineering, vol. 14, no. 1, pp. 46–53, 2026. doi: 10.11648/j.jeee.20261401.15

[5] A. I. Kawoosa, D. Prashar, M. Faheem, and N. K. Jha, "Using machine learning ensemble method for detection of energy theft in smart meters," IET Generation, Transmission & Distribution, 2023. doi: 10.1049/gtd2.12997

[6] S. Zidi, A. Mihoub, S. M. Qaisar, M. Hafeez, and A. Derhab, "Electricity theft detection in smart grids using machine learning," Frontiers in Energy Research, vol. 12, p. 1383090, 2024. doi: 10.3389/fenrg.2024.1383090

[7] F. G. Yem Souhe et al., "A novel smart method for state estimation in a smart grid using smart meter data," Applied and Computational Intelligence and Soft Computing, 2022, Art. no. 1–14.

[8] M. N. Hasan et al., "An efficient electricity theft detection based on deep learning," Scientific Reports, vol. 15, 2025. doi: 10.1038/s41598-025-93140-z

[9] B. Jayabalan, R. K. Yadav, R. Batra, and A. K. Saxena, "An innovative neural network-based technique for identifying power quality issues," Multidisciplinary Science Journal, 2024. doi: 10.29073/msj.v7i1.2597

[10] D. Wang and W. Liu, "Deep Learning Detection of Inaccurate Smart Electricity Meters: An LSTM-CNN Approach," IEEE Transactions on Smart Grid, 2022. [Online]. Available: https://par.nsf.gov/servlets/purl/10324621

[11] C. F. Mbey et al., "Fault detection and classification using deep learning method and neuro-fuzzy algorithm in a smart distribution grid," The Journal of Engineering, 2023. doi: 10.1049/tje2.12324

[12] F. Shehzad et al., "Deep learning-based meta-learner strategy for electricity theft detection," Frontiers in Energy Research, vol. 11, 2023.

[13] Q. Huang et al., "A novel electricity theft detection strategy based on dual-time feature fusion and deep learning methods," Energies, vol. 17, p. 275, 2024.

[14] S. Abdulkareem et al., "Machine intelligence aware electricity theft detection for smart metering applications," Waves in Random and Complex Media, 2023. doi: 10.1080/17455030.2023.2239368

[15] Z. Liu, Y. Wang, Q. Wang, and M. Hu, "Vision transformer-based anomaly detection in smart grid phasor measurement units using deep learning models," IEEE Access, vol. 13, pp. 44565–44576, 2025. doi: 10.1109/ACCESS.2025.3549679

[16] P. Khetarpal, N. Nagpal, P. Siano, and M. Al-Numay, "Power quality disturbance signal segmentation and classification based on modified BI-LSTM with double attention mechanism," IET Generation, Transmission and Distribution, vol. 18, pp. 50–62, 2024. doi: 10.1049/gtd2.13065

[17] Z. Wang, H. Zhang, X. Liu, and S. Chen, "Deep Reinforcement Learning for the Detection of Abnormal Data in Smart Meters," Sensors, vol. 22, no. 21, p. 8543, 2022. doi: 10.3390/s22218543

[18] N. Javaid et al., "Non-technical losses detection using autoencoder and bidirectional gated recurrent unit to secure smart grids," IEEE Access, vol. 10, pp. 56863–56875, 2022. doi: 10.1109/ACCESS.2022.3178226

[19] M. Abdel-Basset, N. Moustafa, and H. Hawash, "Privacy-preserved generative network for trustworthy anomaly detection in smart grids: A federated semisupervised approach," IEEE Transactions on Industrial Informatics, vol. 19, no. 1, pp. 995–1005, 2022.

[20] M. M. Buzau et al., "Pattern-based and context-aware electricity theft detection in smart grid," Sustainable Cities and Society, 2022. doi: 10.1016/j.scs.2022.103994

[21] M. M. Badr et al., "Efficient and Accurate Zero-Day Electricity Theft Detection from Smart Meter Sensor Data Using Prototype and Ensemble Learning," Sensors, 2025.

[22] R. Xia et al., "An attention-based wide and deep CNN with dilated convolutions for detecting electricity theft considering imbalanced data," Electric Power Systems Research, vol. 214, p. 108886, 2023.

[23] J. Wang et al., "Detection of distributed photovoltaic electricity theft against adversarial evasion attacks," Electrical Engineering, Springer, 2025. doi: 10.1007/s00202-025-03332-z

[24] A. Takiddin, M. Ismail, and E. Serpedin, "Robust data-driven detection of electricity theft adversarial evasion attacks in smart grids," IEEE Transactions on Smart Grid, vol. 14, no. 1, pp. 663–676, 2022.

[25] M. Wen et al., "FedDetect: A Novel Privacy-Preserving Federated Learning Framework for Energy Theft Detection in Smart Grid," IEEE Internet of Things Journal, vol. 9, pp. 6069–6080, 2022. doi: 10.1109/JIOT.2021.3113146

[26] M. H. Zafar et al., "Step towards secure and reliable smart grids in industry 5.0: A federated learning assisted hybrid deep learning model for electricity theft detection using smart meters," Energy Reports, vol. 10, pp. 3001–3019, 2023.

[27] [Author group], "A privacy-preserving heterogeneous federated learning framework with class imbalance learning for electricity theft detection," Applied Energy, 2024. doi: 10.1016/j.apenergy.2024.124172

[28] Z. Jiang et al., "Introducing edge intelligence to smart meters via federated split learning," Nature Communications, vol. 15, 2024. doi: 10.1038/s41467-024-53352-9

[29] J. Jithish, B. Alangot, N. Mahalingam, and K. S. Yeo, "Distributed anomaly detection in smart grids: a federated learning-based approach," IEEE Access, vol. 11, pp. 7157–7179, 2023.

[30] M. F. Guato Burgos, J. Morato, and F. P. Vizcaíno Imacaña, "A review of smart grid anomaly detection approaches pertaining to artificial intelligence," Applied Sciences, vol. 14, no. 3, p. 1194, 2024.