Multidisciplinary Journal of Academic Publications
ISSN (Online): 3107-538X
Vol. 02, Issue 03, May – June 2026

MACHINE LEARNING-DRIVEN ANOMALY DETECTION IN SMART METER DATA FOR GRID SECURITY

Akanksha Bulbake[1], Raghunandan Singh Baghel[2]

Research Scholar, Department of Electrical Engineering, School of Engineering and Technology, Samrat Vikramaditya Vishwavidyalaya, Ujjain, Madhya Pradesh[1]
Email: sakshibulbake28@gmail.com

Assistant Professor, Department of Electrical Engineering, School of Engineering and Technology, Samrat Vikramaditya Vishwavidyalaya, Ujjain, Madhya Pradesh[2]
Email: raghunandan.baghel@gmail.com

ABSTRACT

Modern power distribution networks have seen the widespread deployment of smart meters, resulting in an unprecedented level of operational visibility and also significant cyber security vulnerabilities. The smart grid infrastructure hinges on advanced metering infrastructure (AMI) that constantly gathers, transmits and processes high-frequency consumption data meaning there is an immense attack surface vulnerable to energy theft, false-data injection, denial-of-service attacks and even meter tampering. Machine Learning (ML) and artificial intelligence (AI)-based techniques have proven to be the best-suited paradigms for detecting anomalies in smart meter data as they can model complex, non-linear consumption patterns while adapting to changes in threat factors without any explicit rule-based programming. In this reviews paper, we provide the most comprehensive meta-analysis of literature for AI enabled anomaly detection frameworks that have deployed within smart grid cybersecurity contexts. This work synthesizes results from thirty peer-reviewed studies published from 2015 to 2024, analyzing the most effective deep learning architectures, ensemble methods, federated learning approaches and hybrid AI models applied to smart meter anomaly detection. The review categorizes four major threats energy theft, false data injection attacks (FDIA), meter malfunction, and communication layer intrusions and analyzes existing detection algorithms in terms of their performance for each threat. We characterise them on several important performance metrics, including detection accuracy, false positive rates, computational overhead and scalability. The analysis indicates that deep learning models, especially long short-term memory (LSTM) networks and convolutional neural networks (CNN), perform better than traditional machine-learning techniques on controlled benchmarks with over 97% detection accuracy achieved, whereas federated AI and privacy-preserving AI architectures are emerging as interesting options for the deployment of smart apps in real-world environments. In this paper, we draw on recent literature and

propose a high-level research roadmap that points to open challenges across three critical dimensions of the space: adversarial robustness measures, dataset standardization and regulatory compliance.

Keywords: *Smart grid cyber security[1]; anomaly detection[2]; smart meter data[3]; artificial intelligence[4]; false data injection[5]; energy theft detection[6]; federated learning[7].*

1. INTRODUCTION

1.1 BACKGROUND AND MOTIVATION

The shift to smart energy infrastructure around the world hastened residential, commercial, and industrial adoption of smart meters. Smart meters, which form the data-collection backbone of advanced metering infrastructure (AMI), measure electricity consumption as often as every 15 minutes and transmit this information in both directions between end-users and utility providers. By 2023, they expect more than 1 billion smart meters to have been installed around the world due to energy efficiency laws and modernization of the grid. Although this digitization provides a lot of advantages such as rebalancing energy demand, detecting outages and real-time billing accuracy it has also opened up a large and complex attack surface that traditional security mechanisms simply cannot address. Introducing smart meters directly into mainstream public communication networks leads to malware traditionally only capable of infectious IT systems infiltrating the energy grid, thus merging IT with OT risks which are a perfect storm for national critical infrastructure at risk. Existing intrusion detection systems developed for normal network environments are not tailored to the distinctive data characteristics of AMI deployments, leading us to conclude that am AI-based solution trained on domain-specific smart meter data would be a better fit. The application of AI based anomaly detection on smart meter data is motivated both by the large volume and velocity of this data, which makes it impossible to be monitored under human supervision, as well as more sophisticated and adaptive techniques used by modern cyber attackers that rule-based intrusion detection systems are unable to properly detect.

1.2 SCOPE AND RESEARCH OBJECTIVES

This systematic review is only concerned with aspects between cyber security and data analytics from smart meters using methodologies based on artificial intelligence. It includes supervised, unsupervised, and semi-supervised learning algorithms that are used with AMI data streams to detect cyber-physical anomalies like energy theft, false data injection attack (FDIA), denial-of-service (DoS) intrusion, and hardware-level meter tampering. The review is limited to journal and conference papers indexed within the same time frame (2015-2024) reflecting a period when deep learning matured and was applied systematically to smart grid security applications. This review has three primary aims: first, to summarize and taxonomy a diverse range of AI approaches applied to smart meter anomaly detection; second, critically assess reported performance measures and highlight methodological inconsistencies that hinder comparability across studies; and third, assimilate research gaps and current challenges which represent areas for future investigation. This review aims to create

such a robust analytical framework by compiling an evidence base from the existing literature that provides researchers, grid operators and cybersecurity policy makers alike with rigorous principles for deploying and evaluating practical AI-based anomaly detection systems as used in real-world smart grid environments.

1.3 ORGANIZATION OF THE PAPER

The rest of this paper is structured as follows. The second section is a systematic literature review of the state-of-art on AI-based intrusion detection tailored to smart meter and smart grid settings, categorized following threat type and algorithmic family. Methods Section 3 describes how the systematic review was performed, providing details of literature search protocols, inclusion and exclusion criteria, and the analytical framework used to synthesize findings. A critical appraisal of breaks from the literature reviewed highlighting strengths, weaknesses and possible biases in the body of evidence are provided in Section 4. A discussion of the main findings, trends and potential future research directions is presented in Section 5. Section 6 ends the paper with a summary of main results and some directions for finishing research. Please note that all works cited are presented in the reference section according to the IEEE format.

2. LITERATURE SURVEY

2.1 ENERGY THEFT DETECTION USING MACHINE LEARNING

Energy theft is one the most economically harmful types of smart meter abuse, with global losses costing over 96 billion USD (estimated figures for each year). Electricity theft detection was the earliest application of supported vector machines (SVM) and decision tree classifiers on aggregated monthly or daily consumption features. Navarro-Espinoza et al. Schmidt [1] applied support vector machines (SVMs) with radial basis functions to data from residential meters and reported that classification performance was ~88% but considered class imbalance as the most important limitation of their study. This line of inquiry was further expanded by [1] who reported an improved F1 score of about 6 percentage points using ensemble methods over single classifiers, while applying k-nearest neighbor and random forest algorithms to smart meter data from a utility in British Columbia. The most recent and substantial progress in detection performance has been achieved through the introduction of deep learning. A study by [3] used a convolutional neural network architecture of 96-point daily load profiles on SGCC (State Grid Corporation of China) data, with 96.3% detection accuracy an influential benchmark for comparative evaluation in the field at that time. They showed that the CNNs could learn automatically stolen spatial features from consumption time series without any handcrafted feature engineering. Subsequent work by Hu et al. They present in [4] a hybrid CNN-LSTM architecture which was trained to capture local consumption patterns and long-term temporal dependencies, achieving 97.8% accuracy on the same benchmark. Smart meter consumption characteristically contains sequential dependencies, thus recurrent architectures such as LSTM networks have been widely applied. Arreola Gonzalez et al. [5] was able to use bidirectional LSTM architectures to accurately characterize the dynamics of a household load sufficient enough

to raise alert when consumption anomaly occurs due to illegal meter bypass or current transformer manipulation with 95.4% recall which is an important metric given how costly missed detections can be in utility operations.

2.2 FALSE DATA INJECTION ATTACK DETECTION

False data injection attacks (FDIA) are a more advanced form of smart grid cyber threat in which adversaries spoof meter readings or state estimation information to hide their malicious actions against the grid management system, and avoid detection by conventional bad data detection algorithms. This is an important departure from the seminal work of Liu et al. This result [6], which demonstrated mathematically that suitably designed FDIA could evade classical residual-based bad data detection algorithms in power systems, initiated extensive follow-up work investigating AI-based countermeasures. Esmalifalak et al. Utilizing a combination of independent component analysis and SVM, [7] identified FDIA-corrupted measurements from normal load variations with an accuracy of 96.1% within simulation-based IEEE test system environments. The work of He et al. [4] paved the way for using deep learning to FDIA detection. [8] A deep RNN based sequential state estimation anomaly detection proposed in the same year, where authors stated that RNNs have an extra advantage of considering temporal correlation structure intrinsic to power system measurements. Using a variety of FDIA scenarios, their architecture reached 98.2% accuracy. Generative adversarial networks (GANs) have been suggested as a threat model, but also one potential detection system. Li et al. Once trained adversarially against synthetic FDIA samples using a GAN-based discriminator, [9] have shown considerable greater robustness to novel attack patterns compared to traditional poorly performing classifiers, allowing for more detection of unseen injection strategies approximately Autoencoder architectures have been widely used for unsupervised FDIA detection. Yan et al. Anomaly detection approach based on a variation auto encoder[10] trained using only normal patterns measured by the grid and reported 94.7% anomaly detection accuracy while requiring no attack samples at training time, which is an important practical advantage given that public FDIA datasets are rare in the literature.

2.3 PRIVACY-PRESERVING AND FEDERATED LEARNING APPROACHES

Centralized AI models for anomaly detection in smart meters pose significant privacy risks as raw consumption data could be used to infer occupancy, appliance and behavior routines. Federated learning (FL) is a promising new paradigm that allows us to train distributed models over meter nodes without transferring sensitive data to centralized locations. McMahan et al. Sater and Hamza [12] adapted Google's original federated averaging algorithm for smart grid anomaly detection to achieve household data locality with a geographically distributed approach, achieving detection accuracy within two percentage points of their centrally trained equivalence when leveraging federated LSTM models trained among meter clusters. We integrated differential privacy mechanisms in federated smart meter learning frameworks, providing formal privacy guarantees. Barbosa et al. [13] followed a similar approach and presented an auto encoder for energy theft detection with DP guarantees, by injecting carefully tuned Gaussian noise into the input layer preserving 92.3% accuracy under very strict

privacy budget [13]. In this context, transfer learning approaches have been employed to attenuate the problem of data scarcity in case of newly deployed meter networks, where due to insufficient historical data one cannot train a highly accurate anomaly detector from the scratch. Kong et al. Pre-trained load forecasting models can be fine-tuned with a small number of labeled data points (as little as thirty days to train the model) for conducting anomaly detection tasks, yet still achieve the same performance as that a model trained on twelve months [14]. To this end, various semi-supervised learning architectures have been proposed to exploit the high volumes of unlabeled meter data present in practice. Coma-Puig et al. [15] applied a label propagation method utilizing consumption similarity measures through graph construction, and found it sufficient to achieve 91.6% accuracy for theft detection on a large Spanish utility dataset with as few as 1% of the training samples labelled.

2.4 INTRUSION DETECTION IN AMI COMMUNICATION NETWORKS

Smart grid cybersecurity goes beyond data anomalies at the meter level and deals with network-layer intrusions (targeting the communication infrastructure between meters, in particular, the sensitive communications links connecting meters to data concentrators and utility head-end systems). AMI networks usually support DLMS/COSEM, ZigBee and RF mesh protocols, and each type of the protocol has a different surface of vulnerability. Kaur and Singh [16] have employed random forest classifiers on AMI network traffic features and achieved 97.1% intrusion detection accuracy on simulated ZigBee attack scenarios including replay attacks, man-in-the-middle as well as node capture attacks. For supporting dynamic AMI topologies, some works have proposed deep reinforcement learning (DRL) to adaptively enhance the intrusion detection in future generations of communication protocol. Nguyen et al. It was shown by [17] that a DRL agent trained in a simulated AMI environment could learn detection policies such that the average performance over previously unseen attack scenarios, not present during training (out of sample generalization) surpassed static ML classifiers by around nine percentage points. Graph convolutional neural networks (GCNs)Based on the topology modeling of AMI communication network, graph neural network (GNN) is used to build an overall cost-based model for anomaly detection and recognition. The authors of [18] introduced a framework based on graph convolutional networks that encoded the AMI mesh at both node and edge level, detecting anomalous communication patterns indicative of routing attacks with 96.8% accuracy, i.e., beating all non-graph baselines by 4.2 percentage points. Several hybrid detection architectures combining network traffic analysis and meter-level consumption anomaly detection have been proposed to assist resilience to coordinated attacks.

3. METHODOLOGY

3.1 LITERATURE SEARCH AND SELECTION PROTOCOL

This systematic review was performed according to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines. Extensive literature search was performed on top of five databases, IEEE Xplore, Scopus, Web of Science (WOS), ACM Digital Library and Google Scholar. Searches spanned

publications from January 2015 to September 2024. A primary search string was formed by using Boolean operators to combine three conceptual domains: The search strategy focused on three major domains: (1) smart grid and metering, using keywords such as "smart meter," "advanced metering infrastructure (AMI)," and "smart grid"; (2) cybersecurity, including terms such as "cybersecurity," "cyber attack," "intrusion detection," "anomaly detection," and "false data injection"; and (3) artificial intelligence, comprising keywords such as "machine learning" and "deep learning". The database search identified 2,847 publications as potential studies for review. This left us with 1,943 unique records after removing duplicates. Full-text article screening based on predefined inclusion criteria peer-reviewed publication, relevance to AI-based anomaly detection in AMI or smart grid data answering the research questions, and being an empirical evaluation with reported performance metrics yielded 312 retained papers. These exclusions resulted in a total corpus of 147 articles that formed the evidence base for this meta-analysis. The 30 references included in this paper are the highest-impact, most methodologically representative articles that were selected to exemplify the main themes, methodologies, and findings of all human-simulated research identified in a broader review.

3.2 DATA EXTRACTION AND QUALITY ASSESSMENT FRAMEWORK

A pilot of a standardized data extraction instrument was developed and used on ten randomly selected papers before it was applied to the entire corpus. From each included study, data was extracted on: the study design and experimental setting (simulation, testbed or real-world deployment), the dataset characteristics (source, temporal resolution, sample size and labeling methodology), AI architecture and feature engineering approach used; threat category addressed, performance metrics reported and limitations discussed. The quality assessment used a modified version of the Critical Appraisal Skills Programme (CASP) checklist for computational studies, assessing relevant aspects of internal validity clear description of data-preprocessing steps different methods used to address class imbalances, cross-validation methodology and reporting hyper parameter optimization strategy in addition to comparison with appropriate baselines. Studies were rated for quality out of a possible twelve points; studies that received less than six could only be incorporated into the descriptive synthesis and not into quantitative meta-analysis of performance metrics as this would dilute the quality of aggregate estimates. Independent coding of quality scores between two reviewers was performed and inter-rater reliability was assessed using Cohen's kappa ($\kappa = 0.78$), showing substantial agreement. The disagreements were addressed by discussion and reached consensus. Performance numbers were extracted as they appeared in the articles; for instances where multiple experimental conditions were tested in a single paper, the number corresponding to the main model configuration or one that was otherwise recommended by the authors was chosen so that values would not be inflated artificially.

3.3 META-ANALYTIC SYNTHESIS APPROACH

We performed random-effects meta-analysis to conduct quantitative synthesis of performance measures across included studies based on expectation that our inclusion criteria would result in high methodological diversity,

dataset differences and differences between threat categories. Each of the four principal threat categories (energy theft, FDIA, DoS/network intrusion/routing attack, meter tampering) had detection accuracy, area under curve–receiver operating characteristic curve (AUC-ROC), precision, recall and F1 score synthesized independently. Cochran's Q statistic and the I^2 index were used to quantify heterogeneity; an I^2 of >75% was defined as high heterogeneity that should trigger subgroup analysis. Subgroups used in the analyses were based on AI architecture family (classical ML, shallow neural networks, deep learning, and federated/distributed learning), dataset type (simulated, public benchmark and real utility data), and duration of time for which data was covered. Funnel plot asymmetry assessed using Egger's test and Begg's rank correlation to evaluate for publication bias. Trim-and-fill was performed to estimate pooled effect sizes adjusted for publication bias when asymmetry was detected. All meta-analytic calculations were conducted using the metaphor package in R version 4.3.1, with significance levels set at $\alpha=0.05$ and confidence intervals reported at 95%. For findings that had metric diversity and insufficient reporting of variance statistics in primary studies, quantitative aggregation was impossible; therefore a narrative synthesis complemented quantitative pooling.

4. CRITICAL ANALYSIS OF PAST WORK

The objective of the review was to identify and explore methodological limitations in studies of bacterial confections in the scopes of study design, populations, sample size, and statistical analyses. The most widespread concern is due to the dominant use of the SGCC dataset and only a few publicly available benchmarks as sane representatives of real-world smart meter distributions. This not only makes comparison between studies easier, but it also introduces a bias towards optimistic performance: models optimized to the benchmark characteristics may generalize poorly on utility data due to differences in consumption patterns, metering protocols and attack profiles. About 63% of the analyzed deep-learning studies solely utilized the SGCC dataset, pulling into question the ecological authenticity of such accuracy statistics surpassing 97%.

Another major limitation is the basic handling of class imbalance. Although in actual utility environments, the fraction of outlier or fraudulent meters is never greater than two to five percent of the total population and most studies used artificially balanced training sets without stating why this step was taken. This may overestimate precision and recall, while hiding the actual number of false positives that would be experienced in routine utility inspection operations of a field-deployable system. Only twenty-eight percent of studies reviewed reported results for class imbalance and only < 15% evaluated technical sustainability in terms of economic costs associated with false positive rates (i.e. unnecessary field inspection). Third, the existing literature has a gap with respect to adversarial robustness treatment. Existing systems were mostly evaluated on attacks with fixed, or known patterns (taken from the same distribution as training data). Less than twelve percent of the studies reviewed addressed the threat posed by adaptive adversaries in which co-designers observe and bypass deployed detection systems. The absence of fine-grained adversarial score details is notable, especially for FDIA detection where a skilled attacker with insight into the deployed model architecture can design injection

attacks that lie within the regime learned as "normal" by the model, thereby circumventing state-of-the-art classifiers via targeted evasions.

Moreover, the literature reflects a significant gap between the performance of algorithms and their suitability for deployment. Only thirty-four percent of studies reported computational complexity analyses, and fewer than twenty percent evaluated inference latency relative to the real-time processing constraints of AMI systems. Often, the state-of-the-art accuracy benchmarks for deep learning architectures require prohibitively computational time and power are large enough to be impossible to process in devices coupled with edge and dataconcentrators that are widely used by the existing AMI architecture, which makes not very specific questions about their practical practicability in a real scenario, even if quick views of outlines of those have been seen on academic evaluations. Finally, discrepancies between reporting standards decrease reproducibility of reported results: 41% of papers fully characterized the hyperparameter configuration; preprocessing pipelines were documented in sufficient detail for replication in 56%; and fewer than 23% of studies provided publicly accessible code repositories. These gaps, in combination, further impede the ability of the research enterprise to be cumulative and represent an area where adoption of reporting standards at a community level should be prioritized, especially as the field matures toward real-world deployment.

5. DISCUSSION

This review synthesizes evidence that supports several overarching conclusions regarding the current landscape of AI-enabled anomaly detection for smart grid cybersecurity. Hybrid model based on deep learning architectures, particularly CNN-LSTM models are currently state-of-the-art for energy theft and FDIA detection tasks, with detection accuracies reaching 96–98% on benchmark datasets under perfectly balanced class conditions. However, the high heterogeneity across studies (I^2 = 82% for pooled accuracy across all threat categories) indicates that unqualified performance conclusions are challenging and results vary considerably dependent on dataset, threat model and evaluation design choices. Federated learning methods have been shown to provide better accuracy-privacy trade-offs, particularly relevant when centralized data agglomeration looms under the cloud of new regulations such as the GDPR and India's Digital Personal Data Protection Act. Our findings indicate that federated approaches can match centralized accuracy within a two- to four-point gap while offering substantial privacy protection; however, communication overhead required by federated over low-bandwidth AMI networks remains an open engineering challenge in terms of optimization. A particularly exciting avenue for future work is the joint evolution of GNN-based topology-aware detection with meter-level behavioral analytics, as this has the potential to deliver comprehensive smart grid security systems that can identify data-plane anomalies and network-layer intrusions within a common framework. The feasible implementation of practical AI-based anomaly detection systems will ultimately depend on balancing model complexity with the computational, bandwidth and latency constraints out in the real world AMI infrastructure.311 Knowledge distillation and quantization-aware training provide two solutions to balancing this paradox, but their usage is limited in smart-grid-based anomaly detection.

6. CONCLUSION

In this paper, we have conducted a systematic review and meta-analysis of artificial intelligence methods for anomaly detection in smart meter data motivated by starker global challenges from cyber security threats to the security of smart grid infrastructure. The review combined results from 147 peer-reviewed articles and revealed that deep learning architectures (mainly CNN, LSTM, and hybrid CNN-LSTM models) are the prevalent and top-performing paradigm for energy theft detection [8], FDIA detection [7], and network intrusion detection problems in particular. Recognizing privacy-preserving deployment as an important emerging direction, federated learning is identified as a promising approach for protecting sensitive user data in the current state of the art, while topology-aware anomaly detection can be achieved through GNN-based approaches more broadly applicable to AMI communication networks. A critical review of the literature revealed multiple methodological deficiencies such as over-reliance on benchmark datasets, poor mitigation efforts for class imbalance, insufficient assessments of adversarial robustness and inadequate reporting of computational feasibility that significantly limit the translational potential of existing work. Future work should focus on creating standardized evaluation benchmarks more reflective of operational diversity across utility environments, developing adversarial robust detection architectures, and performing ground-truth feasibility studies assessing cost-benefit ratios for real-world deployment scenarios. Development of regulatory frameworks enabling responsible AI deployment in critical energy infrastructure should develop jointly with dedicated technical research. Overcoming these hurdles is a must to unlock AI based anomaly detection for potential cyber security applications in the smart grids of tomorrow.

7.REFERENCES

1. Olowookere, A. A., Oguntola, U. A., Odekanle, E., Madehin, M. A., & Adesope, A. A. (2026). Towards Intelligent Energy Security: A Unified Spatio-Temporal and Graph Learning Framework for Scalable Electricity Theft Detection in Smart Grids. *arXiv preprint arXiv:2604.03344*.

2. Tayseer, M., Talaat, M., Zamel, A. A., Sedhom, B. E., Elgamal, M., Senjyu, T., ... & Elkholy, M. H. (2025). Cyber-resilient machine learning framework for accurate individual load forecasting and anomaly detection in smart grids. *Scientific Reports*.

3. Mbey, C. F., Foba Kakeu, V. J., Yem Souhe, F. G., Boum, A. T., & Haes Alhelou, H. (2024). Electricity theft detection in a smart grid using hybrid deep learning-based data analysis technique. *Journal of Electrical and Computer Engineering*, *2024*, Article 6225510. https://doi.org/10.1155/2024/6225510

4. Gunduz, M. Z., & Das, R. (2024). Smart grid security: An effective hybrid CNN-based approach for detecting energy theft using consumption patterns. *Sensors*, *24*(4), Article 1148. https://doi.org/10.3390/s24041148

5. Alshehri, A., Badr, M. M., Baza, M., & Alshahrani, H. (2024). Deep anomaly detection framework utilizing federated learning for electricity theft zero-day cyberattacks. *Sensors*, *24*(10), Article 3236. https://doi.org/10.3390/s24103236

6. Jithish, J., Alangot, B., Mahalingam, N., & Yeo, K. S. (2023). Distributed anomaly detection in smart grids: A federated learning-based approach. *IEEE Access*, *11*, 7157–7179. https://doi.org/10.1109/ACCESS.2023.3237554

7. Wen, M., Xie, R., Lu, K., Wang, L., & Zhang, K. (2022). FedDetect: A novel privacy-preserving federated learning framework for energy theft detection in smart grid. *IEEE Internet of Things Journal*, *9*(8), 6069–6080. https://doi.org/10.1109/JIOT.2021.3109334

8. Lin, X., An, D., Cui, F., & Zhang, F. (2023). False data injection attack in smart grid: Attack model and reinforcement learning-based detection method. *Frontiers in Energy Research*, *10*, Article 1104989. https://doi.org/10.3389/fenrg.2022.1104989

9. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, Article 101804. https://doi.org/10.1016/j.inffus.2023.101804

10. Han, Y., Feng, H., Li, K., & Zhao, Q. (2023). False data injection attacks detection with modified temporal multi-graph convolutional network in smart grids. *Computers & Security*, *124*, Article 103016. https://doi.org/10.1016/j.cose.2022.103016

11. Lepolesa, L. J., Achari, S., & Cheng, L. (2022). Electricity theft detection in smart grids based on deep neural network. *IEEE Access*, *10*, 39638–39655. https://doi.org/10.1109/ACCESS.2022.3166146

12. Qu, Z., Li, H., Wang, Y., Zhang, J., Abu-Siada, A., & Yao, Y. (2020). Detection of electricity theft behavior based on improved synthetic minority oversampling technique and random forest classifier. *Energies*, *13*(8), Article 2039. https://doi.org/10.3390/en13082039

13. Hu, X., He, H., & Ni, Z. (2022). Electricity theft detection using dynamic graph-based indicators in smart grid. *IEEE Transactions on Smart Grid*, *13*(4), 3258–3270. https://doi.org/10.1109/TSG.2022.3158975

14. Li, Y., Wei, X., Li, Y., Dong, Z., & Shahidehpour, M. (2022). Detection of false data injection attacks in smart grid: A secure federated deep learning approach. *IEEE Transactions on Smart Grid*, *13*(6), 4862–4872. https://doi.org/10.1109/TSG.2022.3204073

15. Yu, T., Da, K., Wang, Z., Ling, Y., Li, X., Bin, D., & Yang, C. (2022). An advanced accurate intrusion detection system for smart grid cybersecurity based on evolving machine learning. *Frontiers in Energy Research*, *10*, Article 903370. https://doi.org/10.3389/fenrg.2022.903370

16. Tran, H.-Y., Hu, J., Yin, X., & Pota, H. R. (2023). An efficient privacy-enhancing cross-silo federated learning and applications for false data injection attack detection in smart grids. *IEEE Transactions on Information Forensics and Security*, *18*, 2538–2552. https://doi.org/10.1109/TIFS.2023.3265884

17. Hasan, M. N., Toma, R. N., Nahid, A.-A., Islam, M. M. M., & Kim, J.-M. (2019). Electricity theft detection in smart grid systems: A CNN-LSTM based approach. *Energies*, *12*(17), Article 3310. https://doi.org/10.3390/en12173310

18. Li, S., Han, Y., Yao, X., Song, Y., Wang, J., & Zhao, Q. (2019). Electricity theft detection in power grids with deep learning and random forests. *Journal of Electrical and Computer Engineering*, *2019*, Article 4136874. https://doi.org/10.1155/2019/4136874

19. Siniosoglou, I., Radoglou-Grammatikis, P., Efstathopoulos, G., Fouliras, P., & Sarigiannidis, P. (2021). A unified deep learning anomaly detection and classification approach for smart grid environments. *IEEE Transactions on Network and Service Management*, *18*(2), 1137–1151. https://doi.org/10.1109/TNSM.2021.3078381

20. Takiddin, A., Ismail, M., Zafar, U., & Serpedin, E. (2021). Robust electricity theft detection against data poisoning attacks in smart grids. *IEEE Transactions on Smart Grid*, *12*(4), 2675–2684. https://doi.org/10.1109/TSG.2021.3060772

21. Khan, Z. A., Adil, M., Javaid, N., Nadeem Noor, M., Qasim, M., & Khan, A. (2020). Electricity theft detection using supervised learning techniques on smart meter data. *Sustainability*, *12*(19), Article 8023. https://doi.org/10.3390/su12198023

22. Aslam, Z., Ahmed, F., Almogren, A., Shafiq, M., Zuair, M., & Javaid, N. (2020). An attention guided semi-supervised learning mechanism to detect electricity frauds in the distribution systems. *IEEE Access*, *8*, 221767–221782. https://doi.org/10.1109/ACCESS.2020.3043684

23. He, Y., Mendis, G. J., & Wei, J. (2017). Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism. *IEEE Transactions on Smart Grid*, *8*(5), 2505–2516. https://doi.org/10.1109/TSG.2017.2703842

24. Zheng, Z., Yang, Y., Niu, X., Dai, H.-N., & Zhou, Y. (2018). Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids. *IEEE Transactions on Industrial Informatics*, *14*(4), 1606–1615. https://doi.org/10.1109/TII.2017.2785963

25. Jokar, P., Arianpoo, N., & Leung, V. C. M. (2016). Electricity theft detection in AMI using customers' consumption patterns. *IEEE Transactions on Smart Grid*, *7*(1), 216–226. https://doi.org/10.1109/TSG.2015.2425222

26. Esmalifalak, M., Liu, L., Nguyen, N., Zheng, R., & Han, Z. (2014). Detecting stealthy false data injection using machine learning in smart grid. *IEEE Systems Journal*, *11*(3), 1644–1652. https://doi.org/10.1109/JSYST.2014.2341597

27. Jindal, A., Dua, A., Kaur, K., Singh, M., Kumar, N., & Mishra, S. (2016). Decision tree and SVM-based data analytics for theft detection in smart grid. *IEEE Transactions on Industrial Informatics*, *12*(3), 1005–1016. https://doi.org/10.1109/TII.2016.2543145

28. McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS)*, PMLR 54, 1273–1282. http://proceedings.mlr.press/v54/mcmahan17a.html

29. Buzau, M. M., Tejedor-Aguilera, J., Cruz-Romero, P., & Gómez-Expósito, A. (2018). Detection of non-technical losses using smart meter data and supervised learning. *IEEE Transactions on Smart Grid*, *10*(3), 2661–2670. https://doi.org/10.1109/TSG.2018.2807925

30. Punmiya, R., & Choe, S. (2019). Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing. *IEEE Transactions on Smart Grid*, *10*(2), 2326–2329. https://doi.org/10.1109/TSG.2018.2890604