Smart Grid Security

Subjects: Engineering, Electrical & Electronic

Contributor: Muhammed Zekeriya Gunduz, Resul Das

In Internet of Things-based smart grids, smart meters record and report a massive number of power consumption data at certain intervals to the data center of the utility for load monitoring and energy management. Energy theft is a big problem for smart meters and causes non-technical losses.

Keywords: convolutional neural network ; cyber security ; deep learning ; energy theft

1. Introduction

The development of the Internet has enabled more effective and widespread use of Internet of Things (IoT) applications. IoT enables the connection of different objects to the Internet and the ability to communicate with devices in distant networks [1]. Critical infrastructures such as electricity grids have become IoT-based [2]. Electricity generation, transmission, distribution, and consumption processes have become more manageable in this way. IoT-based electricity systems are called the smart grid. The advanced metering infrastructure (AMI) is the communication network of smart grid applications [3]. The AMI carries sensitive information, making it a potential target for attackers. Due to the inherent vulnerabilities of communication networks, cyber-security emerges as a leading problem in smart grid systems [4].

The daily life of humankind depends on electricity and requires effective management. AMI helps this management by using control commands and real-time transmission of the data to utilities, customers, and third parties. Generally, an AMI system consists of smart meters, gateways, communication networks, and a headend system [5]. The most prominent component of AMI is smart meters. Smart meters increase the frequency of collection of energy consumption data, enabling advanced data analysis that was not possible before [6]. A smart meter records and transmits energy consumption of the customers at specific intervals for billing and management [7]. Unauthorized access to a smart meter may result in data tampering attacks called energy theft [8]. Energy theft is a significant challenge for smart grid applications as malicious actors continue to exploit potential vulnerabilities [9]. Unethical customers represent the highest probability of threats to the AMI and smart meters. In the past, energy theft mainly involved physical disruptions like cut-offs or damage. However, contemporary instances may encompass sophisticated attacker models, including erasing log events, false data injection (FDI) attacks, intercepting communication, and data manipulation [10].

Energy theft is a significant concern for utilities, and it has emerged as a global issue, resulting in technical and economic losses for operators and governments [11]. Deep learning (DL)-based models play a prominent role in the design of effective intrusion detection systems (IDSs). Such IDSs are used to identify abnormal activities such as FDI and data tampering [12]. Energy theft is an important issue that needs to be solved to improve smart grid applications. Also, information and communication technologies (ICTs) and correlated cyber-threats necessitate proactive measures. There are various studies on energy theft detection handling the consumption data to achieve a high detection rate (DR) and accurate results [13][14][15][16][17]. Many methods are used for energy theft detection, such as statistics, data mining, machine learning (ML), and DL techniques [18]. DL-based IDSs play a critical role in identifying energy theft attacks [19].

2. Smart Grid Security

Many vulnerabilities inherited from communication networks exist in AMI.

Understanding the data flow in smart grid applications is significant, and this can be achieved by examining their general structure. The overall structure of the smart grid environment is shown in **Figure 1**. Energy generated from diverse sources is transmitted over long distances through transmission lines and distributed to consumers via distribution lines. Data transmission is provided through AMI in the context of the energy infrastructure. While the Wide Area Network (WAN) is used in generation and transmission domains, the Neighborhood Area Network (NAN) and Field Area Network (FAN) are used in the distribution domain. Lastly, the Home Area Network (HAN) and Industrial Area Network (IAN) are used in the consumption domain.

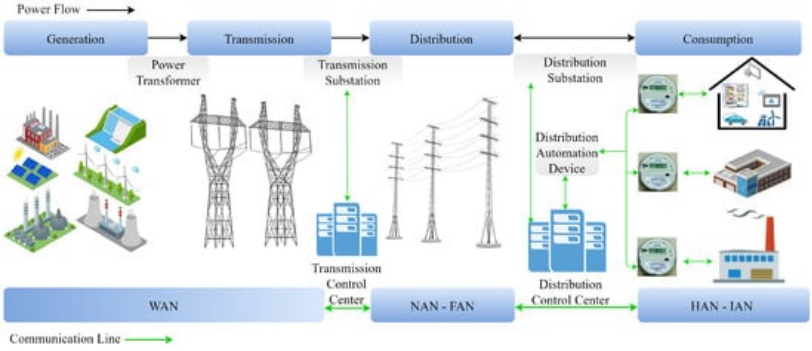

Figure 1. Overall structure of the smart grid environment [20].

Energy theft detection in smart grids has been an active research area in recent years. The literature has introduced various strategies for detecting energy theft. These strategies include state estimation, game theory, and data-driven strategies. Data-driven strategies [21] are more prevalent due to their scalability for handling large systems and their cost-effectiveness in computational resources. Statistics, data mining, ML, and DL are among the prominent data-driven methods extensively employed to extract knowledge from consumption patterns, enabling inferential assessments. While detecting NTLs involves challenges, smart meters allow the extensive storage of energy data, enabling various analytical approaches. This has led to the development of various classification techniques.

Jokar et al. [22] propose an energy theft detector within AMI based on consumption patterns, utilizing the SVM approach. The detector enhances the classification accuracy to 94%. Moreover, it addresses a range of cyber-attack vectors associated with energy theft, and these are widely acknowledged in the literature. The authors of [23] introduced a two-step energy-theft-detection system utilizing DT and SVM, achieving an accuracy of 92.5%. However, there is no information on whether the dataset is balanced or imbalanced. The researchers in [24] present an energy-theft-detection method utilizing ensemble ML models. The concept behind the models involves combining various ML methodologies into a unified predictive model to increase DR and decrease the error rate. The results indicate that a bagging-type ensemble ML approach, which aggregates the outcomes of independent ML models in parallel through averaging, outperforms a boosting approach. However, when compared to other approaches, the recommended model has not demonstrated better success.

Despite the absence of a real dataset in [25], notable achievements in performance were attained through the application of a neural network. They achieved an overall DR of 93%. The authors of [26] have devised a novel approach for identifying and detecting energy theft within distribution systems, employing the multilayer perceptron artificial neural network (MP- ANN). They achieved a successful differentiation between malicious and honest users, averaging a detection rate of 93.4%. However, there is no information on whether the dataset is balanced or imbalanced. In [27], a hybrid deep neural network (DNN) approach is proposed. The gated recurrent unit (GRU) technique was used, which is an evolved variant of LSTM belonging to the category of recurrent neural networks (RNNs). The hybrid DNN combines CNN, GRU, and particle swarm optimization (PSO). However, when compared to other approaches, the recommended hybrid model has not quite demonstrated better accuracy, and the proposed model tends to overfit. The work referenced as [28] employed a deep RNN classifier using GRU to catch temporal correlations within individual customer load profiles, thereby introducing a detector with a DR reaching up to 93%. However, it is not clear whether the dataset is balanced or imbalanced. In [29], the authors present a CNN model to detect energy theft, utilizing the State Grid Corporation of China (SGCC) dataset. They illustrate energy consumption over four weeks for randomly selected honest and malicious consumers. Initially, consumption is displayed by dates and later by weeks. Date-based representation fails to differentiate between honest users and thieves, but the weekly representation distinguishes them. Honest consumers show periodic energy usage, while the thieves display less periodicity. However, there is no information on whether the dataset is balanced or imbalanced. The researchers in [30] presented a hybrid model on energy consumption patterns to detect energy theft with CNN and long short-term memory (LSTM), using the SGCC dataset. The CNN autonomously identified and categorized features, whereas the LSTM managed the sequential nature of the time-based data. The authors solved the imbalanced dataset problem by applying the synthetic minority over-sampling technique (SMOTE) method to augment the NTL class, equalizing it with honest customer counts. While achieving an 89% accuracy, the model demonstrated a lower DR of nearly 87%. Compared to other approaches, the recommended hybrid model has not demonstrated better accuracy. Adil et al. [31] used the CNN-LSTM approach on the SGCC dataset and achieved 87.9% accuracy. However, compared to other approaches, the proposed model is not very satisfactory. Kocaman and Tümen [32] introduced an LSTM classifier for identifying malicious customers. They utilize data selection, normalization, and weight updating as preprocessing steps. The LSTM classifier architecture comprises LSTM cells, dropout layers, $ReLu$ activation functions,

and a softmax classifier. Evaluation involves precision, accuracy, and recall metrics for assessing model performance. However, it is unclear how they resolved the issue of the imbalanced dataset.

The authors in [33] used the Irish Social Science Data Archive (ISSDA) dataset. They employed cluster-based algorithms, specifically the fuzzy Gustafson–Kessel and fuzzy c-means, achieving a 74.1% area under the curve (AUC). However, they achieved low true positive rate (TPR) and high FPR, which are 63.6% and 24.3%, respectively. Lastly, the authors of [34] describe an energy-theft-detection method using data about power provider system consumption at the edge. Centralized data centers employ K-means clustering and DNN to extract features. CNN refines daily, weekly, and monthly patterns. RF at the edge data center classifies the characteristics, speeding up the edge computing processing. This approach is more accurate and computationally efficient than previous methods, making it suitable for edge data centers.

Approaches using only traditional ML models often face challenges in extracting distinct consumption patterns due to the complex structure of power consumption data. This situation leads to low performance and accuracy. On the other hand, DL models can better explore complex structures, thus achieving higher success than ML models. **Table 1** summarizes prominent ML- and DL-based approaches for developing energy theft detectors.

Table 1. Literature overview on energy theft detection based on consumption data.

Ref.	Year	Platform	Proposed Model	Dataset	Accuracy	Presented Main Contribution
[30]	2019	N/A	CNN-LSTM based	SGCC	89	The irregular and abnormal consumption patterns of consumers are analyzed
[33]	2018	N/A	Clustering based	ISSDA	74 (AUC)	Malicious examples are not needed to train the method for future detection
[27]	2020	Python 3.x	CNN-GRU-PSO	SGCC	89	Preprocessing steps, feature selection, feature extraction, and classification are performed using a lot of techniques and the proposed model outperforms imbalancing issue
[26]	2020	N/A	MP-ANN	ISSDA	93.4 (DR)	Self-organizing is used for clustering the consumers according to similar consumption patterns, i.e., classification as honest or malicious. The number of transformers that have suspect consumers is reduced without the need to install measurement units on all transformers
[31]	2020	Python 3.x	CNN-LSTM	SGCC	87.9	An efficient solution to overcome imbalanced data, overfitting, and high-dimensional data limitations is introduced
[23]	2016	N/A	DT-SVM	OpenEnergy	92.5	The newly proposed system exhibits the capability to accurately identify instances of energy theft in real time across all stages of power transmission and distribution
[28]	2018	Python 3.x	GRU (RNN-based)	ISSDA	92.5 (DR)	Temporal patterns are utilized in energy consumption, and a GRU-based RNN enhances detection performance, optimizing hyperparameters through a random search analysis in the learning phase
[22]	2016	N/A	SVM-based	ISSDA	94 (DR)	Six different attack vectors are designed to obtain manipulated consumption data
[24]	2021	Python 3.x	Ensemble ML	ISSDA	90 (AUC)	Data pre-processing is used to address imbalanced data with SMOTE and Near-miss techniques, achieving optimal detection rates through bagging-type ensemble ML demonstrated with diverse consumer samples
[29]	2018	N/A	Wide and Deep CNN	SGCC	80 (AUC)	Unlike existing methods tailored for one-dimensional data, wide and deep CNN handles detecting electricity theft by effectively capturing both periodic and non-periodic consumption patterns in two-dimensional data
[32]	2020	N/A	LSTM-based	SGCC	93.6	A new technique is devised to streamline data, enhancing usability and facilitating the extraction of meaningful insights from the dataset

Ref.	Year	Platform	Proposed Model	Dataset	Accuracy	Presented Main Contribution
[25]	2021	Python 3.x	Neural Network	Grid LabD Tool	93	A novel method is introduced for detecting electricity theft, focusing on “balance attacks” with prosumers manipulating readings for total aggregated balance. A cluster-based detection model is introduced as a middle-ground approach, bridging the gap between using a single model for all users and individual models for each user
[35]	2021	Matlab2019	CNN-WeightedRF	Mathpower Tool	95.71	An FDI intrusion-detection model combining CNN and weighted RF is able to detect the spurious data more accurately compared with other detection models
[36]	2015	N/A	SVM	ISSDA	75.8	The classification models simplify a demand-side management study, analyze tariff methods, and offer insights for policymakers
[37]	2010	VisualBasic	SVM	Tenaga Nasional	60	This work aims to aid Tenaga Nasional Berhad Distribution in Malaysia to reduce NTLs within the distribution sector caused by electricity theft
[38]	2018	Python 3.x	DNN-based	ISSDA	92.6 (DR)	This work proposes a DNN-based customer-specific detector that can mitigate electricity theft cyber-attacks
[39]	2017	N/A	Density-based clustering	ISSDA	93.2	This work exhibits superior performance compared to alternative methods across nearly all categories of theft
[40]	2022	Python 3.x	Attention LSTM Inception	SGCC	95	This work addresses the elevated FPR issue arising from widespread misclassification, leading to financial burdens
[41]	2022	Python 3.x	KTBoost Classifier	SGCC	93.38	Taking into account all minority sample regions in the dataset, the robust-SMOTE technique generates minority class samples with reduced susceptibility to overfitting and the generation of noisy samples
[42]	2023	Python 3.7	Deep-CNN	Researcher-generated	95	The proposed theft detection method, utilizing the SMOTE technique to generate minority class samples with reduced susceptibility to overfitting and noise, attains the highest accuracy compared to all other studied methods
work	2024	Python 3.10	CNN-based	ISSDA	95.34	CNN-based architecture is combined with traditional ML methods. A detector that provides high success in detecting all attack vectors has been designed. The imbalanced data problem was solved using GAN.

Glancing at these noteworthy works, novel CNN-based hybrid models for energy theft detection and proposed a CNN-based deterministic model to detect energy theft based on consumption patterns were studied. CNN automatically captures the distinct features of consumption behaviors from the data. It is very important for the effectiveness of energy-theft-detection models. It was conducted that a comparative analysis using ML and sigmoid classifiers to detect consumption patterns based on extracted features, aiming to enhance detection performance. Hybrid solutions using both CNN and traditional ML methods have been observed to achieve higher TPR and lower FPR compared to pure DL solutions.

References

1. Gunduz, M.Z.; Das, R. Internet of things (IoT): Evolution, components and applications fields. Pamukkale Univ. J. Eng. Sci. 2018, 24, 327–335.
2. Das, R.; Gunduz, M.Z. Analysis of cyber-attacks in IoT-based critical infrastructures. Int. J. Inf. Secur. Sci. 2019, 8, 122–133.
3. Emmanuel, M.; Rayudu, R. Communication technologies for smart grid applications: A survey. J. Netw. Comput. Appl. 2016, 74, 133–148.

4. Kimani, K.; Oduol, V.; Langat, K. Cyber security challenges for IoT-based smart grid networks. Int. J. Crit. Infrastruct. Prot. 2019, 25, 36–49.
5. Gunduz, M.Z.; Das, R. Communication Infrastructure and Cyber-Security in Smart Grids. J. Inst. Sci. Technol. 2020, 10, 970–984.
6. Qays, M.O.; Ahmad, I.; Abu-Siada, A.; Hossain, M.L.; Yasmin, F. Key communication technologies, applications, protocols and future guides for IoT-assisted smart grid systems: A review. Energy Rep. 2023, 9, 2440–2452.
7. Sahoo, S.; Nikovski, D.; Muso, T.; Tsuru, K. Electricity theft detection using smart meter data. In Proceedings of the 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 18–20 February 2015; pp. 1–5.
8. Althobaiti, A.; Jindal, A.; Marnerides, A.K.; Roedig, U. Energy Theft in Smart Grids: A Survey on Data-Driven Attack Strategies and Detection Methods. IEEE Access 2021, 9, 159291–159312.
9. Takiddin, A.; Ismail, M.; Serpedin, E. Detection of Electricity Theft False Data Injection Attacks in Smart Grids. In Proceedings of the 2022 30th European Signal Processing Conference (EUSIPCO), Belgrade, Serbia, 29 August–2 September 2022; pp. 1541–1545.
10. Badr, M.M.; Ibrahem, M.I.; Kholidy, H.A.; Fouda, M.M.; Ismail, M. Review of the Data-Driven Methods for Electricity Fraud Detection in Smart Metering Systems. Energies 2023, 16, 2852.
11. Wang, Y.; Chen, Q.; Gan, D.; Yang, J.; Kirschen, D.S.; Kang, C. Deep Learning-Based Socio-Demographic Information Identification From Smart Meter Data. IEEE Trans. Smart Grid 2019, 10, 2593–2602.
12. Reda, H.T.; Anwar, A.; Mahmood, A. Comprehensive survey and taxonomies of false data injection attacks in smart grids: Attack models, targets, and impacts. Renew. Sustain. Energy Rev. 2022, 163, 112423.
13. Javaid, N.; Gul, H.; Baig, S.; Shehzad, F.; Xia, C.; Guan, L.; Sultana, T. Using GANCNN and ERNET for Detection of Non Technical Losses to Secure Smart Grids. IEEE Access 2021, 9, 98679–98700.
14. Habib, A.A.; Hasan, M.K.; Alkhayyat, A.; Islam, S.; Sharma, R.; Alkwai, L.M. False data injection attack in smart grid cyber physical system: Issues, challenges, and future direction. Comput. Electr. Eng. 2023, 107, 108638.
15. El-Toukhy, A.T.; Badr, M.M.; Mahmoud, M.M.E.A.; Srivastava, G.; Fouda, M.M.; Alsabaan, M. Electricity Theft Detection Using Deep Reinforcement Learning in Smart Power Grids. IEEE Access 2023, 11, 59558–59574.
16. Berghout, T.; Benbouzid, M.; Muyeen, S.M. Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects. Int. J. Crit. Infrastruct. Prot. 2022, 38, 100547.
17. Buzau, M.M.; Tejedor-Aguilera, J.; Cruz-Romero, P.; Gómez-Expósito, A. Detection of Non-Technical Losses Using Smart Meter Data and Supervised Learning. IEEE Trans. Smart Grid 2019, 10, 2661–2670.
18. Abdulaal, M.J.; Ibrahem, M.I.; Mahmoud, M.M.E.A.; Khalid, J.; Aljohani, A.J.; Milyani, A.H.; Abusorrah, A.M. Real-Time Detection of False Readings in Smart Grid AMI Using Deep and Ensemble Learning. IEEE Access 2022, 10, 47541–47556.
19. Lepolesa, L.J.; Achari, S.; Cheng, L. Electricity Theft Detection in Smart Grids Based on Deep Neural Network. IEEE Access 2022, 10, 39638–39655.
20. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. Comput. Netw. 2020, 169, 107094.
21. Chen, J.; Nanehkaran, Y.A.; Chen, W.; Liu, Y.; Zhang, D. Data-driven intelligent method for detection of electricity theft. Int. J. Electr. Power Energy Syst. 2023, 148, 108948.
22. Jokar, P.; Arianpoo, N.; Leung, V.C.M. Electricity Theft Detection in AMI Using Customers' Consumption Patterns. IEEE Trans. Smart Grid 2016, 7, 216–226.
23. Jindal, A.; Dua, A.; Kaur, K.; Singh, M.; Kumar, N.; Mishra, S. Decision Tree and SVM-Based Data Analytics for Theft Detection in Smart Grid. IEEE Trans. Ind. Inform. 2016, 12, 1005–1016.
24. Gunturi, S.K.; Sarkar, D. Ensemble machine learning models for the detection of energy theft. Electr. Power Syst. Res. 2021, 192, 106904.
25. Alromih, A.; Clark, J.A.; Gope, P. Electricity Theft Detection in the Presence of Prosumers Using a Cluster-based Multi-feature Detection Model. In Proceedings of the 2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Aachen, Germany, 25–28 October 2021; pp. 339–345.
26. Souza, M.A.; Pereira, J.L.R.; Alves, G.d.O.; de Oliveira, B.C.; Melo, I.D.; Garcia, P.A.N. Detection and identification of energy theft in advanced metering infrastructures. Electr. Power Syst. Res. 2020, 182, 106258.

27. Ullah, A.; Javaid, N.; Samuel, O.; Imran, M.; Shoaib, M. CNN and GRU based Deep Neural Network for Electricity Theft Detection to Secure Smart Grid. In Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 15–19 June 2020; pp. 1598–1602.
28. Nabil, M.; Ismail, M.; Mahmoud, M.; Shahin, M.; Qaraqe, K.; Serpedin, E. Deep Recurrent Electricity Theft Detection in AMI Networks with Random Tuning of Hyper-parameters. In Proceedings of the 2018 24th International Conference on Pattern Recognition (ICPR), Beijing, China, 20–24 August 2018; pp. 740–745.
29. Zheng, Z.; Yang, Y.; Niu, X.; Dai, H.N.; Zhou, Y. Wide and Deep Convolutional Neural Networks for Electricity-Theft Detection to Secure Smart Grids. IEEE Trans. Ind. Inform. 2018, 14, 1606–1615.
30. Hasan, M.N.; Toma, R.N.; Nahid, A.A.; Islam, M.M.M.; Kim, J.M. Electricity Theft Detection in Smart Grid Systems: A CNN-LSTM Based Approach. Energies 2019, 12, 3310.
31. Adil, M.; Javaid, N.; Qasim, U.; Ullah, I.; Shafiq, M.; Choi, J.G. LSTM and Bat-Based RUSBoost Approach for Electricity Theft Detection. Appl. Sci. 2020, 10, 4378.
32. Kocaman, B.; Tümen, V. Detection of electricity theft using data processing and LSTM method in distribution systems. Sādhanā 2020, 45, 286.
33. Viegas, J.L.; Esteves, P.R.; Vieira, S.M. Clustering-based novelty detection for identification of non-technical losses. Int. J. Electr. Power Energy Syst. 2018, 101, 301–310.
34. Cheng, G.; Zhang, Z.; Li, Q.; Li, Y.; Jin, W. Energy Theft Detection in an Edge Data Center Using Deep Learning. Math. Probl. Eng. 2021, 2021, e9938475.
35. Na, L.; Xiaohui, X.; Xiaoqin, M.; Xiangfu, M.; Peisen, Y. Fake Data Injection Attack Detection in AMI System Using a Hybrid Method. In Proceedings of the 2021 IEEE Sustainable Power and Energy Conference (iSPEC), Nanjing, China, 23–25 December 2021; pp. 2371–2376.
36. Viegas, J.L.; Vieira, S.M.; Sousa, J.M.C.; Melício, R.; Mendes, V.M.F. Electricity demand profile prediction based on household characteristics. In Proceedings of the 2015 12th International Conference on the European Energy Market (EEM), Lisbon, Portugal, 19–22 May 2015; pp. 1–5.
37. Nagi, J.; Yap, K.S.; Tiong, S.K.; Ahmed, S.K.; Mohamad, M. Nontechnical Loss Detection for Metered Customers in Power Utility Using Support Vector Machines. IEEE Trans. Power Deliv. 2010, 25, 1162–1171.
38. Ismail, M.; Shahin, M.; Shaaban, M.F.; Serpedin, E.; Qaraqe, K. Efficient detection of electricity theft cyber attacks in AMI networks. In Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, 15–18 April 2018; pp. 1–6.
39. Zheng, K.; Wang, Y.; Chen, Q.; Li, Y. Electricity theft detecting based on density-clustering method. In Proceedings of the 2017 IEEE Innovative Smart Grid Technologies—Asia (ISGT-Asia), Auckland, New Zealand, 4–7 December 2017; pp. 1–6.
40. Munawar, S.; Khan, Z.A.; Chaudhary, N.I.; Javaid, N.; Raja, M.A.Z.; Milyani, A.H.; Azhari, A.A. Novel FDIs-based data manipulation and its detection in smart meters' electricity theft scenarios. Front. Energy Res. 2022, 10, 1043593.
41. Hussain, S.; Mustafa, M.W.; Ateyeh Al-Shqeerat, K.H.; Saleh Al-rimy, B.A.; Saeed, F. Electric theft detection in advanced metering infrastructure using Jaya optimized combined Kernel-Tree boosting classifier—A novel sequentially executed supervised machine learning approach. IET Gener. Transm. Distrib. 2022, 16, 1257–1275.
42. Haq, E.U.; Pei, C.; Zhang, R.; Jianjun, H.; Ahmad, F. Electricity-theft detection for smart grid security using smart meter data: A deep-CNN based approach. Energy Rep. 2023, 9, 634–643.