International Journal of Computer Science and Information Technology
ISSN: 3005-9682 (Print), ISSN: 3005-7140 (Online) | Volume 3, Number 1, Year 2024
DOI: https://doi.org/10.62051/ijcsit.v3n1.10
Journal homepage: https://wepub.org/index.php/IJCSIT/index

Review of Detection Methods for Abnormal Electricity Consumption Data in Smart Grid

Naiquan Xiao

Henan University of Science and Technology, Luoyang 471000, China

ABSTRACT

The smart grid is an intelligent system of the power grid, which is a communication information support platform based on the coordinated development of the transmission network and various levels of power grids. It is a highly integrated system characterized by informationization, automation, and interactivity of various voltage levels, including transmission and transformation, distribution, and power dispatch. This article summarizes, analyzes, and summarizes the methods for detecting abnormal electricity consumption data in smart grids. It introduces the detection methods for abnormal electricity consumption data based on traditional technology and artificial intelligence technology, analyzes and elaborates on the basic principles and characteristics of each method, summarizes and looks forward to the challenges and future development trends faced by abnormal electricity consumption data detection in smart grids, and provides some reference for subsequent research.

KEYWORDS

Smart grid; Abnormal detection; Artificial intelligence

1. INTRODUCTION

With the rapid development of Internet of Things (IoT) technology and 5G technology, both industrial growth and population increase have significantly escalated electricity consumption, posing relatively higher requirements on the economic efficiency and operational stability of power grid operators. The Fifth Plenary Session of the 18th Central Committee of the Communist Party of China's "13th Five-Year Plan" explicitly states the need to accelerate the development of "Internet Plus" smart power networks, improve electricity interactive services, promote electricity demand-side response, and meet the diverse needs of electricity supply and demand interaction [1].

With the development of the economy, electricity has become an indispensable part of people's daily lives, especially in recent years, where there has been an explosive growth in electricity consumption, making anomaly detection in power usage particularly crucial. At the same time, with the introduction of the concept of the national digital economy, power grid operators have also embarked on the processes of digitization, networking, and intelligence [2]. The digital transformation of power grid operators is essential for achieving efficient, secure, and reliable operation of the power system. Anomalous behaviors within the power grid not only hinder the intelligent development of the grid but also result in significant economic losses, affecting the revenue of power grid operators. While striving to meet the electricity demand and provide the best service to users, power grid operators are facing losses both in technological and non-technological aspects.

During the process of power transmission and distribution, various losses occur, categorized as technical and non-technical losses [3]. Technical losses typically result from energy dissipation in

transmission lines, transformers, and electrical equipment. Non-technical losses mainly stem from improper electricity usage, electricity theft, meter malfunctions, system failures, and similar reasons [4]. It is estimated that illegal electricity usage causes direct economic losses of up to 20 billion RMB annually in China. Therefore, addressing technical and non-technical loss issues has always been one of the key concerns for power grid operators.

Identifying non-technical factors and mitigating the economic losses they cause are primary focuses for power grid operators. Traditional methods of detecting abnormal electricity usage in power grids involve manually monitoring and identifying abnormal electricity consumption for individual devices, followed by dispatching inspection teams to the locations of these devices for further investigation. If there is a significant variation in power consumption, it is considered abnormal. This traditional approach requires considerable time and financial resources, placing additional burdens on power grid operators. Additionally, its efficiency and detection rate are both very low.

The increasing demands for higher efficiency, reliability, and security in the operation of power grid systems, along with the growing attention to the detection of abnormal power usage data, have underscored the necessity for a leap in power grids, termed as smart grids. Smart grids represent the embodiment of intelligence in traditional power grids; they are high-speed, bidirectional communication networks based on electricity, utilizing a range of advanced technologies and methods to ensure the reliable, economical, and efficient operation of grid systems. Smart grids can supply power more efficiently and respond promptly to a wide range of abnormal events, such as detecting abnormal power consumption of devices and implementing corresponding strategies [5].

With the continuous increase in the number of distributed generation resources of renewable energy such as wind, hydro, and solar power, as well as the extensive adoption of various smart terminal devices like intelligent appliances, large volumes of data flow will emerge between power grid operators, electricity users, power equipment, and equipment control centers [6]. Within the entire architecture of smart grids, numerous edge devices accessing networks will generate tens of thousands of pieces of raw power data. These data not only accurately assess the operation of the power grid but also enhance the security, efficiency, and sustainability of the entire power system. Currently, most domestic and foreign researchers believe that the true value of smart grids lies not in improving the efficiency of the interconnected physical devices themselves, but in the wealth of unrefined raw data information they contain and how to efficiently, rapidly, and meaningfully process this information [7]. Consequently, in recent years, the detection of abnormal power data in smart grids has received widespread attention, with issues such as the real-time detection of single-device anomalies and privacy protection of power data among multiple devices in different regions being hotspots and challenges in research.

Despite bringing significant benefits, smart grids still face many technical challenges. Smart grids are vulnerable to various vulnerabilities, such as device node failures, power outages, energy theft, and cyber-attacks, resulting in non-technical losses in the grid [8]. In particular, malicious actors may exploit security vulnerabilities in the grid to launch sophisticated cyber-attacks (such as denial of service, infrastructure damage, and theft of user data) [9], which may disrupt the normal operation of the grid system. According to a recent study, global economic losses due to non-technical losses reach $96 billion annually. Non-technical losses can be identified by monitoring abnormalities in the grid, which are reflected in the power data collected by smart meters.

The widespread adoption of smart meters provides power grid operators with the opportunity to collect vast amounts of electricity usage data. The high-resolution power data collected by smart meters offers insights into electricity consumption in different regions and consumers' lifestyles. However, existing classification schemes suffer from some limitations that restrict detection rates, such as data imbalance issues where the number of normal and abnormal samples is disproportionate. Benign samples are easily obtained through analysis of historical data, whereas abnormal samples are often scarce or absent from the dataset, limiting detection rates. Moreover, detection rates are

influenced by various non-malicious factors, such as dynamic changes in consumer energy demands and the diversity of appliance types. If these non-malicious factors are not properly distinguished and addressed, they may be mistaken for false positives, leading to poor detection performance.

To achieve acceptable detection accuracy and manage large volumes of smart meter data securely and reliably, power grid operators must extend their existing power systems to distributed data centers. In this regard, cloud computing is considered to play a critical role [10]. Cloud computing is a new computing paradigm widely adopted in industry, academic organizations, and individual clients. In smart grids, cloud computing can effectively handle the massive data generated by millions of smart meters deployed across urban areas [11]. Managing massive data and identifying malicious factors in smart grids are highly complex tasks that exceed the processing capacity of existing power systems. Therefore, leveraging cloud computing for storage and computing mechanisms can optimize information processing to achieve higher detection rates [12]. However, the widespread deployment of smart meters and the large volume of electricity usage data pose challenges to the centralized data center processing model. To conserve energy consumption of edge device nodes and reduce unnecessary data transmission, deploying edge data processing centers with data processing capabilities at single-device edge nodes has become a new anomaly detection pattern. In this mode, users' electricity usage data do not need to be uploaded to centralized cloud computing data centers, reducing upload bandwidth.

Anomaly detection of abnormal electricity usage data plays an irreplaceable role throughout the entire power system. In transmission and distribution networks, anomaly detection methods for abnormal electricity usage data can quickly identify various abnormal states and locations, pinpoint the source of anomalies, and prevent the further spread of abnormal states, thus minimizing losses in a timely manner. Using anomaly detection technology for abnormal electricity usage data in terminal smart grid systems can enhance user experience, help power departments and related enterprises save corresponding manpower and operational costs, and ensure the stable operation of the grid in a relatively economical state.

2. DEFINITION AND CLASSIFICATION OF ANOMALOUS DATA

Anomaly Detection (AD) refers to the process of identifying unusual or abnormal behavior, events, or patterns in data. In AD, it is typically assumed that the majority of the data is normal, while anomalies are relatively rare. Anomalies can be sudden events, outliers, errors, faults, or other unusual circumstances. However, anomalies in smart grids may arise from multiple sources, including abnormal consumption patterns from customers, infrastructure failures, power outages, malicious network attacks, or energy theft. Examples of events that can be classified as "anomalies" include power outages, transmission line failures, abnormal power consumption, and both transient and sustained power outages [13]. As shown by [14], there are three main types of anomalies in time series data:

(1) Point anomalies: As shown in Figure 1, point anomalies refer to a single value or a small set of values in a time series that stands out compared to other observations. These outlier values may be temporary noise, often caused by sensor errors or abnormal system operations. Traditional anomaly detection methods typically set upper and lower threshold limits based on previous data, and values exceeding these limits are considered point anomalies.

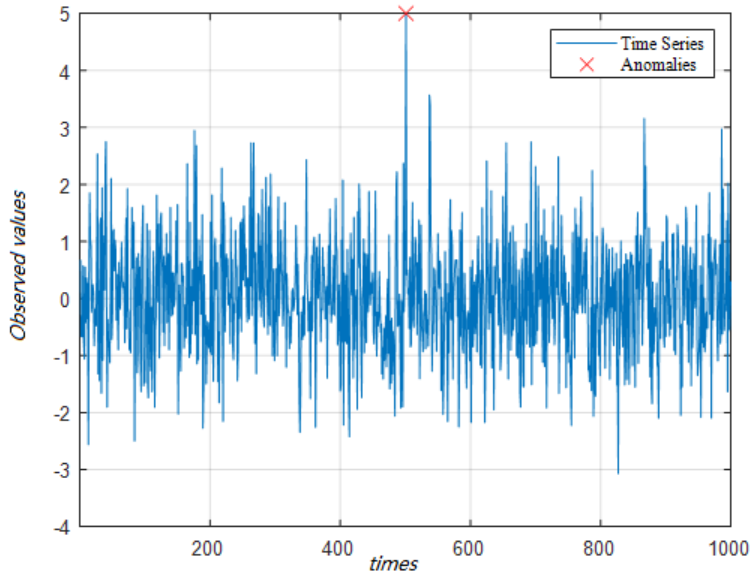

Figure 1. Point anomaly diagram

(2) Contextual anomalies: As shown in Figure 2, contextual anomalies are similar to point anomalies, referring to data points or sequences of values observed within a short time frame that do not exceed predefined threshold values. The values of these anomaly data points may appear within a reasonable range in the overall sequence but deviate from their neighboring data points, thus considered anomalies based on context. These data points deviate from the expected patterns or shapes, making them difficult to detect.

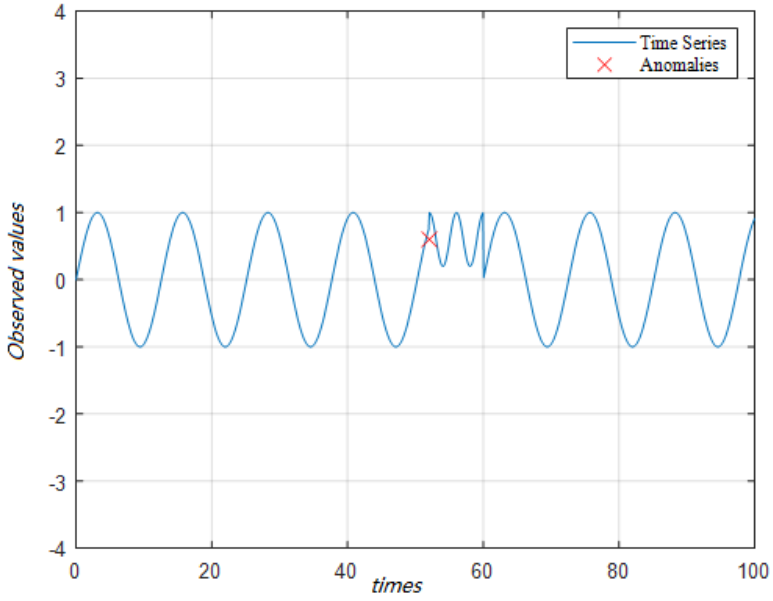

Figure 2. Context anomaly diagram

(3) Collective anomalies or pattern anomalies: As shown in Figure 3, collective anomalies or pattern anomalies refer to a group or series of observations where the values deviate from the overall pattern or periodicity of the sequence. Over time, these anomalous data gradually exhibit patterns different from normal data. While individual values within the anomalies may not appear problematic, collectively, they are different from normal data points. Due to the difficulty in identifying these anomalies all at once, context is particularly important when detecting them in the long term.

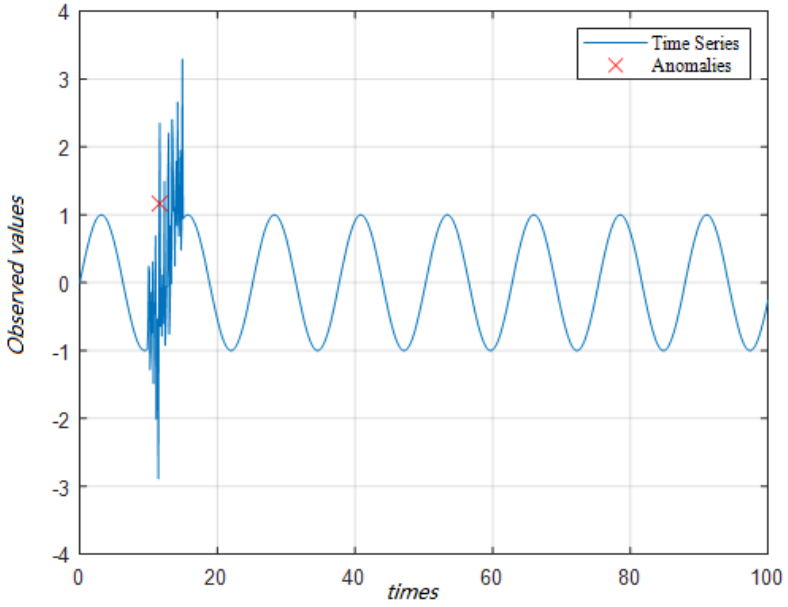

Figure 3. Abnormal group or pattern diagram

2.1. Traditional Methods for Detecting Abnormal Electricity Consumption Data in Traditional Power Grids

Traditional methods for detecting anomalous business data in power grids are proposed based on the characteristics of power grid business data combined with data statistics, which are suitable for specific power systems. The Generalized Extreme Studentized Deviation (ESD) Test [15], also known as the Grubbs's test, is used for detecting outliers in univariate time series that approximately follow a normal distribution. In one application, the authors [16] introduced the ESD test into their work to classify normal and abnormal energy consumptions and then removed the detected anomalies from the historical data for further modeling and forecasting. The authors of [17] also used the ESD test to identify and remove anomalies within the energy consumption dataset of a commercial building in Hong Kong, and then proposed an ensemble method that ultimately achieved good performance on the next-day consumption prediction.

This family of models detects anomalies based on one-step-ahead prediction. For a time series $Y=\{y_1, y_2, ..., y_t\}$, an autoregressive moving average (ARMA) model is $y_t = a_1 y_{t-1} + a_2 y_{t-2} + ... + a_p y_{t-p} + n_t + b_1 n_{t-1} + ... + b_q n_{t-q}$, where n_t represents the error at time step i. Here p is the total number of autoregressive terms, q is the number of lagged errors, and b is the moving average coefficients. An autoregressive integrated moving average (ARIMA) model further accounts for the non-stationary characteristics of certain types of time series and makes the sequence stationary in an initial difference step, in other words, eliminating the trend by subtracting previous values from current values.

Anomaly detection of a load consumption profile of office space was studied in [18]. The authors compared the standard ARIMA model and the neural network (NN)-based ARIMA model in terms of their predictive ability and anomaly detection performance. Since the standard ARIMA model tends to converge towards the mean value in long-term predictions, it failed to capture consumption patterns and was not able to distinguish between normal and anomalous consumption under the two-sigma rule. On the other hand, the non-linear activation layers in the neural network (NN)-based ARIMA enabled the model to capture the long-term consumption pattern and achieved satisfactory prediction accuracy in an 8-week power consumption time series.

2.2. Machine Learning-Based Methods for Anomalous Power Usage Data Detection in Power Grids

2.2.1. Supervised Methods

Anomaly detection can be considered as a classification task in specific scenarios. Supervised classification methods require the training set to have labels. One study [19] focused on detecting false data injections in power flow measurements of the IEEE 118-bus test system using a Gaussian kernel Support Vector Machine (SVM). In this case, the dataset is labeled since the false data injections were simulated by the authors. Another study [20] aimed at detecting anomalous consumption behaviors adopted Google's "micro-moments" concept. It employed a rule-based model to assign "micro-moment" labels to energy consumption data ("normal" labels include "good usage", "turn on device", and "turn off device"; "abnormal" labels include "excessive consumption" and "consumption while outside"), transforming the anomaly detection problem into a classification problem. The authors utilized a deep neural network classifier and achieved high detection accuracy.

2.2.2. Unsupervised Methods

1) Reconstruction-Based Methods

Reconstruction-based anomaly detection is a process of feature extraction or dimensionality reduction, through which an initial raw dataset is reduced to a smaller but more meaningful feature set [21]. During the training phase, reconstruction-based models attempt to extract information about historical patterns from the original time series. In the testing phase, when a new observation arrives, the features of the new data instance are compared to the extracted historical patterns. The greater the deviation from the patterns, the more likely it is to be labeled as an anomaly. Feature reconstruction can facilitate preprocessing and labeling of the original training data and can further be applied to unsupervised anomaly detection or directly used as an anomaly detection scheme.

In a study on network attack detection in large-scale smart grids [22], Symbolic Dynamic Filtering (SDF) was adopted as a feature extraction strategy. The phase space of the original time series was partitioned into a finite number of cells. Subsequently, the time series was compressed into a symbol sequence by assigning a symbol to each partition. This facilitated the subsequent use of Dynamic Bayesian Networks (DBN) to reveal causal relationships among these symbolic features, and Restricted Boltzmann Machines (RBM) to capture the distribution of normal operation in the grid system.

Principal Component Analysis (PCA) is one of the most popular feature extraction methods. It produces a dimensionality-reduced representation of approximately independent features based on the covariance matrix of the time series. In [23], PCA was used as a direct method for detecting anomalies in primary distribution voltage amplitude measurements. The measurement time series was first transformed into a matrix representation, followed by PCA to extract independent features and project the original data into a low-dimensional projection space. Anomaly detection was performed based on the residuals between new observation values and the projection space.

Another descriptive symbolic feature extraction method is Symbolic Aggregate Approximation (SAX), which was proposed for power load anomaly detection in [24, 25]. In the implementation of SAX, the time series is first segmented into intervals, and then a symbol is assigned to each segment based on its average value. This transforms the time series into a low-dimensional discrete representation for further processing and anomaly detection.

2) Cluster-Based Methods

Cluster-based methods model the basic characteristics of data by projecting data instances into higher-dimensional spaces and formulating clusters based on distance measures [26]. Data points close to dense clusters belong to the majority class and are more likely to be normal observations, while data points far from clusters are typically labeled as anomalies.

The K-means clustering algorithm [27, 28] is a popular unsupervised clustering method. It is simple and efficient - given prior knowledge of the number of clusters k, the algorithm iteratively adjusts the positions of k cluster centers based on the distances between data instances and the cluster centers. In [29], k-means clustering was applied to multivariate time series of power consumption for 370 users, and a preliminary set of class labels for consumption patterns was established for each user. This result will aid in the detection of consumption pattern drift in subsequent steps.

Isolation Forest (iForest) [30] is another efficient unsupervised anomaly detection method that can also be used for clustering. In this method, each isolation tree recursively partitions the instance space, and then we calculate the average path length from each data instance to all tree roots. Based on the assumption that the number of anomaly data points is small and different from normal data, it should be relatively easy to distinguish anomaly data from normal data, so anomaly data should be isolated in a few steps by partitioning trees. Therefore, normal data points typically reside in deeper branches of the trees, while anomalies are located closer to the root. Shorter path lengths to the root indicate a higher probability of anomalies. In [31], the authors proposed a pattern-based anomaly detection method based on isolation forest. Power consumption time series were discretized using fixed-length sliding windows. Next, the mean, standard deviation, and trend of each segment were computed as original features, followed by PCA for dimensionality reduction of the feature space. Then, isolation forest was applied to detect anomalies in the reduced dataset, achieving high detection accuracy.

3) Prediction-Based Methods

Prediction-based methods rely on accurate forecasts of future time steps. Recurrent Neural Networks (RNNs) are a class of models particularly suitable for handling sequential data. Long Short-Term Memory (LSTM) RNNs are a type of RNN architecture equipped with input, output, and forget gates, which help address the vanishing gradient problem in ordinary RNNs. They have been applied in various time series prediction tasks and have shown promising performance.

In [30], a prediction-based anomaly detection method for power load data was proposed using RNNs. The LSTM-RNN generates one-step predictions of power load. Subsequently, prediction errors are calculated and compared with the standard deviation of all prediction errors. Performance evaluation is based on the two-sigma rule of normal distribution, where approximately 95% of the data lies within the confidence interval $(-2\sigma, 2\sigma)$. Precision and recall are adopted as evaluation metrics for the model. Other studies on RNN-based anomaly detection models for power grids follow a similar approach but employ different evaluation metrics, including Manhattan distance and edit distance [32], autoencoder reconstruction scores [33], and absolute percentage error [34].

3. FUTURE RESEARCH OUTLOOK

In the realm of detecting anomalous electricity usage data in power grid systems, researchers both domestically and internationally have delved into this issue and proposed numerous solutions. These methods demonstrate promising performance in detecting anomalous data in simulated environments. However, due to the relatively short development time of anomaly detection techniques for electricity usage data in power grids, practical challenges such as application difficulties, data leaks, false positives, and false negatives persist. This paper suggests that in future research, scholars should consider data protection and deeply integrate artificial intelligence technologies widely employed across various domains to develop more secure and intelligent anomaly detection methods for electricity usage data in power grids.

1) The lack of labeled data poses a significant challenge. Most time series data in power grids are unlabeled, lacking explicit indications of whether specific data points are normal or anomalous. This complicates the implementation of classification-based anomaly detection methods. Additionally, the imbalance between normal and anomalous data makes it difficult to thoroughly capture the characteristics of anomalous data points. The scarcity of sufficient anomalous data in intelligent grid

time series obstructs the representation of anomalous categories. Establishing anomaly benchmarks for power grid time series would aid in the development of accurate anomaly detection models.

2) Transfer learning [35] aims to enhance learning performance in the target domain by reusing knowledge learned from the source domain. Recently, it has been applied in various tasks including anomaly detection in surveillance videos, image classification, time series classification, and time series forecasting. Exploring the potential benefits of transfer learning for anomaly detection in power grids would be an intriguing topic for future research, as it could enhance the model's generalization ability when facing new environments. For newly constructed equipment or buildings where sufficient historical data is unavailable, we can leverage prior knowledge extracted from existing labeled datasets or historical data from similar equipment or buildings.

3) Most current models are trained offline using large amounts of historical data, which may not be suitable for real-time online anomaly detection. Real-time detection models lack data at the outset when meter readings are just beginning to be collected. Therefore, investigating how to effectively utilize all available data in real-time would be an interesting research topic.

Generative models have the potential to directly capture the underlying distribution of data and generate new instances, making them a promising approach for our objective. In recent years, models based on Generative Adversarial Networks (GANs) have demonstrated excellent performance in tasks such as realistic time series interpolation, time series generation, and power load forecasting. Following this approach, GAN-based models can be used as real-time data augmentation schemes. Subsequently, synthetic data can be generated in real-time to enhance the current input data.

4. SUMMARY

With the continuous development and widespread adoption of the concept of smart grids, various departments and systems within the power grid generate large amounts of electricity usage data every day. Among them, anomalous electricity usage data can have a significant impact on the stability of the power system, making research on the detection of anomalous electricity usage data in the grid a hot topic.

By adopting accurate and efficient methods to promptly locate and correct abnormal electricity usage data in the grid, on the one hand, it can greatly assist power companies in scientifically and efficiently managing electricity usage, reducing unnecessary resource wastage, lowering transmission costs, and optimizing the rational allocation of electricity resources in the power system, thereby improving the electricity usage experience for users. This paper analyzes and summarizes the commonly used methods for detecting anomalous electricity usage data in the grid from a technical perspective, and provides a reasonable outlook on the possible future research directions for detecting anomalous electricity usage data in power systems.

Traditional methods for detecting abnormal data usually require a large number of state comparisons and estimations, resulting in high time and space complexity, which may not meet the real-time computing requirements of modern smart grids. Anomalous data detection methods based on artificial intelligence technology have made significant advancements in detection speed and accuracy, effectively avoiding false positives and false negatives. However, they require a massive amount of real data for model training, which may raise data security concerns. This paper summarizes the definition of anomalies in time series data, discusses classical methods for anomaly detection in power grid time series, and machine learning-based techniques, and proposes three potential future research directions. In the pursuit of reliability and operational efficiency in power grids, anomaly detection will continue to play a key role. With the latest developments in ensemble learning, transfer learning, and generative modeling providing new opportunities to address current challenges, we expect anomaly detection models to become more refined and accurate in applications involving time series data in smart grid environments.

REFERENCES

[1] Gopstein A, Nguyen C, O'Fallon C, et al. NIST framework and roadmap for smart grid interoperability standards, release 4.0[M]. Gaithersburg, MD, USA: Department of Commerce. National Institute of Standards and Technology, 2021.

[2] Hashmi M, Hänninen S, Mäki K. Survey of smart grid concepts, architectures, and technological demonstrations worldwide[C]//2011 IEEE PES conference on innovative smart grid technologies Latin America (ISGT LA). IEEE, 2011: 1-7.

[3] de Souza Savian F, Siluk J C M, Garlet T B, et al. Non-technical losses: A systematic contemporary article review[J]. Renewable and Sustainable Energy Reviews, 2021, 147: 111205.

[4] Chi X, Yan C, Wang H, et al. Amplified locality-sensitive hashing-based recommender systems with privacy protection[J]. Concurrency and Computation: Practice and Experience, 2022, 34(14):

[5] Zhong W, Yin X, Zhang X, et al. Multi-dimensional quality-driven service recommendation with privacy-preservation in mobile edge environment[J]. Computer Communications, 2020, 157: 116-123.

[6] Dileep G. A survey on smart grid technologies and applications[J]. Renewable Energy, 2020, 146: 2589-2625.

[7] Liu Y, Guo W, Fan C I, et al. A practical privacy-preserving data aggregation (3PDA) scheme for smart grid[J]. IEEE Transactions on Industrial Informatics, 2018, 15(3): 1767-1774.

[8] Hammerschmitt B K, da Rosa Abaide A, Lucchese F C, et al. Non-technical losses review and possible methodology solutions[C]. Proceedings of the 6th International Conference on Electric Power and Energy Conversion Systems (EPECS). IEEE, 2020: 64-68.

[9] Gunduz M Z, Das R. Cyber-security on smart grid: Threats and potential solutions[J]. Computer Networks, 2020, 169: 107094.

[10] Xu X, Mo R, Dai F, et al. Dynamic resource provisioning with fault tolerance for data-intensive meteorological workflows in cloud[J]. IEEE Transactions on Industrial Informatics, 2019, 16(9): 6172-6181.

[11] Zhou C, Li A, Hou A, et al. Modeling methodology for early warning of chronic heart failure based on real medical big data[J]. Expert Systems with Applications, 2020, 151: 113361.

[12] Li J, Cai T, Deng K, et al. Community-diversified influence maximization in social networks[J]. Information Systems, 2020, 92: 101522.

[13] Lipčák P, Macak M, Rossi B. Big data platform for smart grids power consumption anomaly detection[C]. 2019 Federated Conference on Computer Science and Information Systems (FedCSIS). IEEE, 2019: 771-780.

[14] Cook A A, Mısırlı G, Fan Z. Anomaly detection for IoT time-series data: A survey[J]. IEEE Internet of Things Journal, 2019, 7(7): 6481-6494.

[15] B. Rosner, "Percentage points for a generalized esd many-outlier procedure," Technometrics, vol. 25, no. 2, pp. 165–172, 1983.

[16] X. Li, C. P. Bowers, and T. Schnier, "Classification of energy consumption in buildings with outlier detection," IEEE Transactions on Industrial Electronics, vol. 57, no. 11, pp. 3639–3644, 2009.

[17] C. Fan, F. Xiao, and S. Wang, "Development of prediction models for next-day building energy consumption and peak power demand using data mining techniques," Applied Energy, vol. 127, pp. 1–10, 2014.

[18] J.-S. Chou and A. S. Telaga, "Real-time detection of anomalous power consumption," Renewable and Sustainable Energy Reviews, vol. 33, pp. 400–411, 2014.

[19] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," IEEE Systems Journal, vol. 11, no. 3, pp. 1644–1652, 2017.

[20] Y. Himeur, A. Alsalemi, F. Bensaali, and A. Amira, "A novel approach for detecting anomalous energy consumption based on micro-moments and deep neural networks," Cognitive Computation, vol. 12, no. 6, pp. 1381–1401, 2020.

[21] S. Khalid, T. Khalil, and S. Nasreen, "A survey of feature selection and feature extraction techniques in machine learning," in 2014 science and information conference. IEEE, 2014, pp. 372–378.

[22] H. Karimipour, A. Dehghantanha, R. M. Parizi, K.-K. R. Choo, and H. Leung, "A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids," IEEE Access, vol. 7, pp. 80 778–80 788, 2019.

[23] A. A. Imayakumar, A. Dubey, and A. Bose, "Anomaly detection for primary distribution system measurements using principal component analysis," in 2020 IEEE Texas Power and Energy Conference (TPEC). IEEE, 2020, pp. 1–6.

[24] M. Yue, "An integrated anomaly detection method for load forecasting data under cyberattacks," in 2017 IEEE Power Energy Society General Meeting, 2017, pp. 1–5.

[25] M. Yue, T. Hong, and J. Wang, “Descriptive analytics-based anomaly detection for cybersecure load forecasting,” IEEE Transactions on Smart Grid, vol. 10, no. 6, pp. 5964–5974, 2019.

[26] A. A. Cook, G. Mısırlı, and Z. Fan, “Anomaly detection for iot timeseries data: A survey,” IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6481–6494, 2020.

[27] J. A. Hartigan and M. A. Wong, “Algorithm as 136: A k-means clustering algorithm,” Journal of the royal statistical society. series c(applied statistics), vol. 28, no. 1, pp. 100–108, 1979.

[28] A. K. Jain, “Data clustering: 50 years beyond k-means,” Pattern recognition letters, vol. 31, no. 8, pp. 651–666, 2010.

[29] G. Fenza, M. Gallo, and V. Loia, “Drift-aware methodology for anomaly detection in smart grid,” IEEE Access, vol. 7, pp. 9645–9657, 2019.

[30] F. T. Liu, K. M. Ting, and Z.-H. Zhou, “Isolation forest,” in 2008 Eighth IEEE International Conference on Data Mining, 2008, pp. 413–422.

[31] W. Mao, X. Cao, T. Yan, Y. Zhang et al., “Anomaly detection for power consumption data based on isolated forest,” in 2018 International Conference on Power System Technology (POWERCON). IEEE, 2018, pp. 4169–4174.

[32] Z. Fengming, L. Shufang, G. Zhimin, W. Bo, T. Shiming, and P. Mingming, “Anomaly detection in smart grid based on encoder-decoder framework with recurrent neural network,” The Journal of China Universities of Posts and Telecommunications, vol. 24, no. 6, pp. 67–73, 2017.

[33] J. Pereira and M. Silveira, “Unsupervised anomaly detection in energy time series data using variational recurrent autoencoders with attention,” in 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), 2018, pp. 1275–1282.

[34] V. Q. Nguyen, L. Van Ma, J.-y. Kim, K. Kim, and J. Kim, “Applications of anomaly detection using deep learning on time series data,” in 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech). IEEE, 2018, pp. 393–396.

[35] D. Wu, B. Wang, D. Precup, and B. Boulet, “Multiple kernel learningbased transfer regression for electric load forecasting,” IEEE Transactions on Smart Grid, vol. 11, no. 2, pp. 1183–1192, 2019.