International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

Power electronics anomaly detection and diagnosis with machine learning and deep learning methods: A survey

Hossein Rahimighazvini [1,*], Zeyad Khashroum [1], Maryam Bahrami [2] and Milad Hadizadeh Masali [1]

[1] *Department of Electrical Engineering, Lamar University, Beaumont, TX 77710, USA.*
[2] *Department of Industrial Engineering, Lamar University, Beaumont, TX 77710, USA.*

International Journal of Science and Research Archive, 2024, 11(02), 730–739

Publication history: Received on 30 January 2024; revised on 13 March 2024; accepted on 16 March 2024

Article DOI: https://doi.org/10.30574/ijsra.2024.11.2.0428

Abstract

Power electronics pertains to the conception, regulation, and utilization of electronic power circuits to proficiently administer and transform electrical energy. Power electronics play a crucial role in maintaining the reliability, efficiency, and security of complex production systems. Also, increasingly important in various applications such as renewable energy systems, electric vehicles, and industrial automation. However, modern power electronics systems are vulnerable to both cyber and physical anomalies due to the integration of information and communication technologies. So far, different methods have been used to detect abnormalities. This survey provides an overview of the state-of-the-art in anomaly detection in power electronics using machine learning and deep learning methods. It highlights the potential of these techniques in addressing the growing complexity and vulnerability of power electronics systems.

Keywords: Power electronics; Anomaly detection; Anomaly diagnosis; Machine learning; Deep learning

1. Introduction

Power electronics is a field that deals with the design, development, and implementation of electronic systems that control and convert electrical power [1, 2]. Power electronics is used in various applications, including smart grids, electric transportation, robotics, and power generation systems [3]. The production of renewable energy has increased due to the progress of power electronics. Converters play a major role in increasing renewable energy sources and storage units. As these converters are used in Photovoltaic (PV) power plants, wind farms, and electric vehicles, to increase operational reliability, they need to improve [4]. Also, the use of power electronics technology in the infrastructure of Internet-based communication networks provides the possibility of coordinated control and increases energy efficiency and flexibility in smart networks. Subsequently, connectivity and integration of power electronics and Internet-based communication networks will lead to potential cyber threats [5, 6]. Therefore, to increase security and reliability, anomaly detection strategies are needed.

Anomaly refers to a deviation from normal conditions or a discrepancy that is not considered satisfactory. It can be anything that does not align with the expected or standard behavior, indicating a potential issue or irregularity [7]. Anomalies can indicate critical incidents, such as technical glitches, or changes in consumer behavior [8]. Abnormalities in consumer conduct can manifest as unforeseen patterns of electricity usage. For example, if a residential area has a stable and predictable pattern of energy consumption during certain hours, a sudden deviation from this pattern can indicate an abnormality[9].

Anomaly detection in power electronics involves the task of identifying and addressing abnormal behavior or deviations from normal operation. Anomaly can occur in various components such as converters, inverters, and power supplies

* Corresponding author: Hossein Rahimighazvini

[10]. Anomaly detection is essential to maintain complex systems, such as power electronic systems, by ensuring full coverage and minimal response time across all platforms, operating systems, and data centers [11]. This essentiality is because anomalies can result in system downtime, decreased efficiency, and higher maintenance expenses [12]. Furthermore, there is a growing need for real-time anomaly detection and classification systems in power electronic systems due to the integration of various technologies like renewable energy sources, smart grids, and cyber-physical systems [10]. This integration adds complexity to electronic power systems, leading to challenges in real-time anomaly detection and necessitating the advancement of sophisticated anomaly detection and classification systems [13].

Machine learning algorithms are increasingly used to automate anomaly detection, and make it more efficient and accurate[14]. Some of these applications including:

- ***Cybersecurity:*** Employing machine learning to identify anomalous activity or intrusions into networks, as well as other cyber-attacks [15].
- ***Fraud detection:*** The process of identifying abnormal trends in financial transactions and fraudulent activity by applying machine learning algorithms [16].
- ***Predicting equipment failures***: This technique forecasts failures and faults in electrical and electronic devices and industrial machinery [17].
- ***Health monitoring:*** Tracking system and equipment performance and health using machine learning algorithms to spot anomalies and possible problems [18].

Machine learning and deep learning algorithms have become increasingly popular in addressing anomaly detection in power electronics. These algorithms can analyze historical data, recognize patterns, and identify anomalies that may not be detectable using traditional methods [2, 19]. It is necessary to create a taxonomy for various anomaly types to choose the appropriate techniques for anomaly detection [20].

This survey presents classified methods in anomaly detection and investigates diagnosis in power electronics with machine learning and deep learning. It is important to notice that while anomaly detection and anomaly diagnosis are related concepts in power electronics, they are distinct from each other. Anomaly detection involves identifying patterns within data that deviate from predicted behaviors [21]. However, the act of diagnosing anomalies involves determining the root cause of an anomaly or deviation from normal behavior [22].

The rest of this paper is organized as follows. Section 2 is a taxonomy of anomalies in power electronics. Section 3 details the approaches that detect anomalies. Section 4 investigates the anomaly diagnosis. Finally, Section 5 concludes the paper.

2. Anomaly Taxonomy

The term "anomaly" or "outlier" can be divided into three categories according to the problem, which are described in the following:

- ***Point anomalies:*** Occurs when data samples exhibit substantial deviation from the norm or expected behavior within a dataset [23]. For example, in the field of power electronics, a sudden drop or increase in the level of voltage in an electrical system is considered a point anomaly [12].
- ***Contextual anomalies:*** These kinds of anomalies might be classified as normal or anomalous depending on the surroundings and situations around them [24]. Temperature readings are one type of data point that could be normal in one context but anomalous in another. For example, an 80°F temperature in the summer could be regarded as normal, but in the winter it might be anomalous. In the same vein, 40°F can be regarded as normal in the winter but anomalous in the summer. Therefore, whether temperature readings are regarded as normal or anomalous depends on the season they are considered (summer vs. winter) [25].
- ***Collective anomalies:*** Collective anomalies manifest when a specific group of data points deviates significantly from the overall dataset. While individual data points may not be considered abnormal on their own, their collective occurrence forms an anomalous pattern [26, 27]. For instance, abnormal power consumption patterns in a group of devices or equipment can be considered collective anomalies [28].

Moreover, various abnormalities that can occur in power electronic systems include the following:

- ***Cyber-attacks:*** Malicious actions are with the objective of disrupting, causing damage to, or gaining unauthorized entry into power electronic systems. These actions include injecting false data, manipulating control signals, or compromising communication networks [29].

- ***Physical faults:*** Defects or failures that impact the components or parameters of power electronic systems. Examples of such faults include over voltages or overheating [30].
- ***Environmental disturbances:*** External factors that exert an influence on the performance or operation of power electronic systems. These factors may include noise, temperature, humidity, solar power, wind speed [31].

3. Anomaly detection techniques in power electronics

Approaches for detecting and categorizing data samples that differ from a data set's normal patterns are known as anomaly detection techniques [7]. Anomaly detection techniques in power electronics can be categorized as supervised, unsupervised, or statistical techniques as shown in Figure 1.

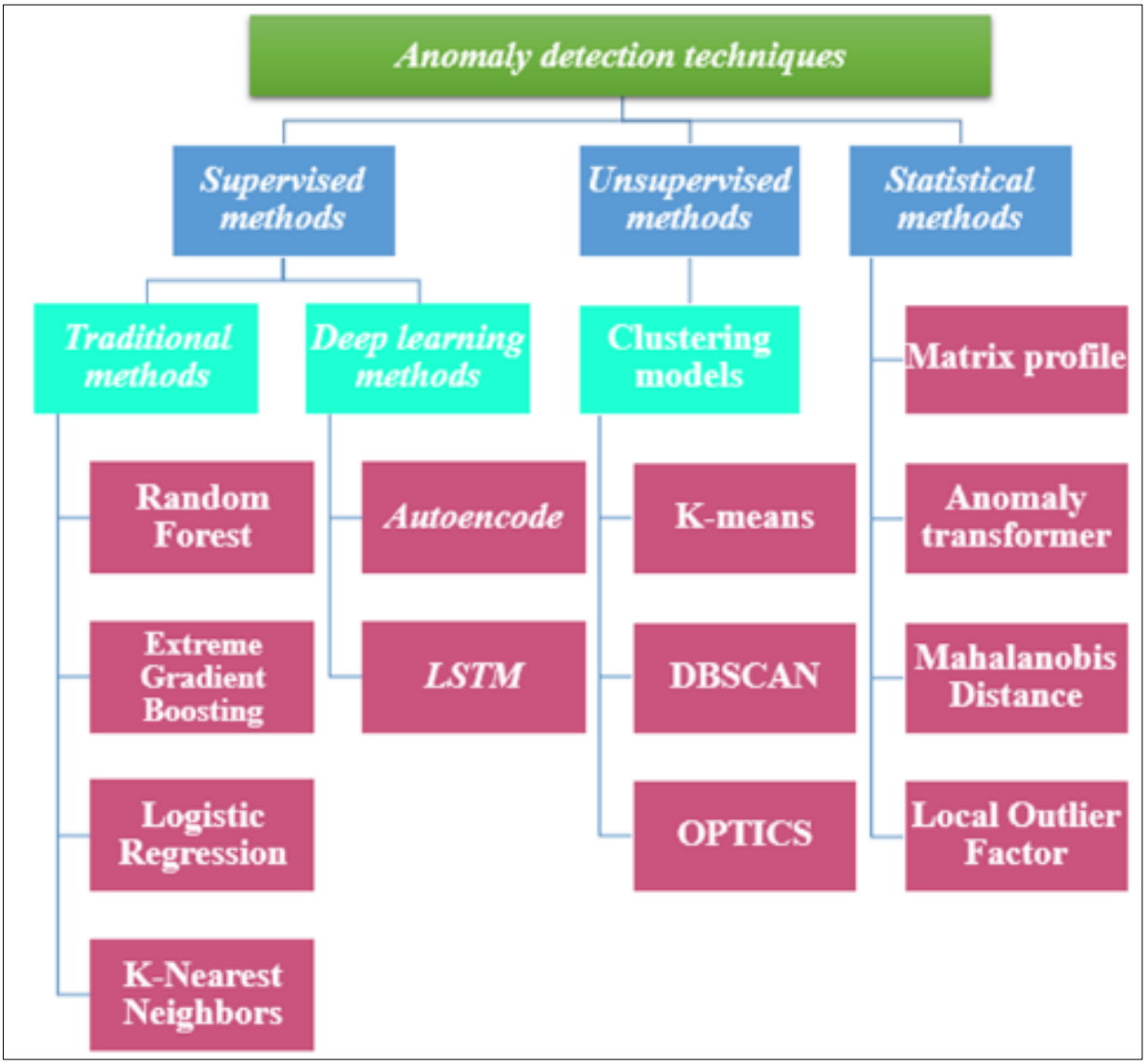

Figure 1 Anomaly detection techniques in power electronics

3.1. Supervised anomaly detection

In the techniques that fall into this category, the training dataset has two types of labels "normal" and "abnormal" [10]. For anomaly detection, a model is built to predict normal and abnormal data, then this model is used to determine the class of unseen data [25]. The lower number of abnormal data compared to normal data, as well as the accurate labeling especially for abnormal classes, are challenges in these techniques [21].

3.1.1. Traditional machine learning methods

The machine learning is a field that grants computers the ability to acquire knowledge through data and make predictions or decisions [32]. In various studies, machine learning algorithms have been used to detect anomalies in power electronics.

The [33] study, introduces a new algorithm for the detection of anomaly presence, classification of the anomaly type, and identification of the origin of the anomaly. By employing an anomaly detection index, anomalies that surpass the $\chi 2$-test are effectively detected. Subsequently, the machine learning algorithms, namely Random Forest (RF), Extreme Gradient Boosting (XGB) algorithms, Logistic Regression (LR), and K-Nearest Neighbors (KNN), are employed for the purpose of classifying anomalies and determining their origin.

Waveforms have been used to train anomaly detection models in power electronics [34]. Waveforms are a form of information that symbolize the alteration of a quantity as time progresses, for instance, voltage, current, or frequency [35]. The [36] study aim is anomaly detection for real electronic signal data from particle accelerator power systems using machine learning algorithms. This study uses real-time series datasets collected from the High Voltage Converter Modulators (HVCM) of the Spallation Neutron Source (SNS) facility. These datasets contain waveform signals collected from the operation of more than 15 HVCM systems during 2020-2022.

3.1.2. Deep learning methods

Recent studies use deep learning methods especially autoencoder models for anomaly detection. The autoencoder is a type of neural network that is appropriate for detecting anomalies as it is trained to reestablish ordinary patterns and displays substantial reconstruction error when confronted with anomalous data [19, 37]. The application of autoencoder models in power electronics anomaly detection is founded upon their capacity to comprehend intricate patterns within the data and discern deviations from the standard behavior, thus serving to enhance the durability and dependability of power electronics systems [38, 39]. Also, the Recurrent AutoEncoders (RAE)-based neural network architectures and recurrent neural networks such as Long-Short-Term-Memory (LSTM) have been proposed for early detection of anomalies in power signals and their application has been proven in the field [37].

As previously achieved [40], a hybrid deep learning approach has been utilized for the detection of anomalies in Electrical Power Steering (EPS) sensor data. In the present study, the model is initially trained on EPS data employing an automatic encoder to extract and compress features. Subsequently, these extracted features are inputted into the LSTM network in order to capture the pertinent dependencies among them. In the [41] study, an LSTM-based anomaly detection model is proposed, which is trained using the Point of Common Coupling (PCC) data of the inverters, frequency, voltage and Rate Of Change Of Frequency (ROCOF). As such, it enables real-time anomaly detection and classification for low-inertia Power Electronics Dominated Grid (PEDG). The study of [42] investigated the use of RAE-based neural network for automatic detection of abnormalities in order to reduce HVCM system failures. Additionally, the study involved training bi-directional Gated Recurrent Unit (GRU), bi-directional LSTM, and convolutional LSTM (ConvLSTM) using real experimental signals, and comparing their performance with other classical anomaly detection methods. Also, the [43] study, has introduced anomaly detectors for electricity theft cyberattack detection in Advanced Metering Infrastructures (AMIs). They use deep (stacked) autoencoders with an LSTM-based Sequence-to-Sequence (seq2seq) structure to design detectors.

The primary limitation associated with the utilization of autoencoder models resides in their susceptibility to overfitting, thereby resulting in suboptimal generalization capabilities when applied to unfamiliar datasets [37]. To address this problem, it is crucial to utilize an adequate amount of training data and implement methods like regularization, dropout, or early termination in the training phase. Furthermore, it is vital to assess the model's performance on a distinct test dataset to verify its ability to effectively adapt to new data [44].

In training deep learning models, there should be a balance between training and generalization [45]. If this balance is not achieved and the training is not appropriate, the model will not perform well when tested on new data that have different distributions than the training data [46]. In the problem of anomaly detection, when the abnormal data have a different distribution from the normal data, the model cannot correctly detect the new abnormal data. Therefore, the value of the loss function increases due to model misclassification [11]. Another disadvantage of the deep learning models is that it require a lot of labeled training data to improve accuracy in classification models [47].

3.2. Unsupervised anomaly detection

This approach does not require labeled data to detect anomalies [48]. In this approach, usually, normal samples are much more than abnormal samples in the test data set. But, if there are more abnormal samples, the predictive model will have a high false alarm rate [21].

The unsupervised anomaly detection approach relies on clustering methods to identify anomalies [5]. Clustering methods group data based on similarities or differences and allow the detection of abnormal or outlier patterns [49]. Some of the clustering algorithms that have been employed to identify anomalies in power electronics include:

- **K-means:** This algorithm partitions the data into k clusters based on the distance to the centroid of each cluster. The K-means assumption is that the normal data samples are positioned near the center of the cluster, while the anomalies are located outside the center [25].
- **DBSCAN:** This algorithm groups the data based on the density of its neighborhood. This algorithm does not force every data instance to belong to a cluster [50].
- **OPTICS:** This algorithm arranges the data points in order of their reach distance, which represents the minimum distance required to connect two points in a cluster. Points that belong to the same cluster are in close proximity to each other, while points that are farther apart have greater reach distances [51].

The [52] has utilized these three methodologies to address the detection of abnormality in electricity consumption for public street lighting. These algorithms facilitate the detection of anomalies by identifying data points that do not pertain to any cluster or exhibit low density. As per the reported outcomes, K-means exhibits the shortest execution time, although the DBSCAN algorithm surpasses both K-means and OPTICS in terms of accuracy in identifying anomalies.

In [53], the Meanshift clustering method utilizes grid-tied inverters and solar-irradiance to perform pre-classification and anomaly detection on time series data pertaining to electrical parameters. The authors in [5] focus on both real-time anomaly detection and classify the type of anomaly. In this research, anomaly detection is done using a new algorithm called Informative Leveraging for Anomaly Detection (ILAD). Also, to classify the types of anomalies, they have employed a novel clustering method called Multivariate Functional Principal Component Analysis (MFPCA).

3.3. Statistical Methods

Statistical techniques employed in power electronics encompass the utilization of mathematical and probabilistic tools to scrutinize and formulate models, and enhance the efficacy, dependability, and efficiency of power electronic systems [54]. The employment of statistical methods can prove advantageous in addressing the challenges posed by the presence of uncertainties, variances, and disturbances that have an impact on power electronic systems; these challenges may take the form of noise, faults, or cyber-attacks [55].

The matrix profile algorithm and anomaly transformer are two statistical methods used for anomaly detection. Power electronic signals and other time series data can be detected using these methods [12]. The Mahalanobis Distance (MD) technique is employed for the detection of anomalous behavior in electronic commodities through the comparison of MD values against baseline values [56]. Moreover, the Local Outlier Factor (LOF) algorithm is another method that is based on statistics and utilized for anomaly detection. The anomaly score produced by this method indicates data points that are outside the average range in the dataset [57].

Table 1 provides a summary of the detection methods that were investigated for anomaly detection.

Table 1 Comparing different methods

Ref.	Year	Category	Method
[52]	024	Unsupervised	K-means, OPTICS, DBSCAN
[41]	2023	Supervised	LSTM
[5]	2023	Unsupervised	Multivariate Functional Principal Component Analysis (MFPCA)

[57]	2022	Statistical	Local Outlier Factor
[33]	2022	Supervised	RF, XGB, LR, KNN
[40]	2022	Supervised	Autoencoder + LSTM
[12]	2022	Statistical	matrix profile algorithm + anomaly transformer
[42]	2022	Supervised	RAE-based neural network + GRU + Bi-LSTM + convolutional LSTM (ConvLSTM)
[43]	2022	Supervised	deep (stacked) auto-encoders with a LSTM-based Sequence-to-Sequence (seq2seq) structure
[53]	2020	Unsupervised	Meanshift clustering

4. Anomaly Diagnosis

Anomaly diagnosis in power electronics entails the procedure of discerning and categorizing abnormal behaviors or faults that affect the components or parameters of power electronics systems, such as converters, inverters, rectifiers, and controllers [58]. Anomaly diagnosis facilitates the comprehension of the fundamental reason behind the abnormality and the implementation of suitable rectifying measures to tackle the matter [59].

By effectively diagnosing anomalies, it is possible to prevent equipment failures, optimize performance, and enhance the overall operation of power electronic systems [60]. The applications of anomaly diagnosis in power electronics include condition monitoring of power electronic devices, predictive maintenance of electrical systems, fault isolation, and detection in power converters [61].

It is worth noting that in [5], anomaly detection is defined as a problem that aims to differentiate between cyber-attacks and physical faults. For instance, the device-level Power Electronics Converters (PEC) have two major anomaly types that are cyber-attacks and physical faults. Although these two types of anomalies are prevalent, distinguishing between cyber-attacks and physical faults is difficult [29]. To tackle this challenge, researchers have put forth various techniques aimed at distinguishing cyber-attacks from physical faults in power electronic systems.

The [30] study, uses a non-invasive anomaly diagnosis mechanism to distinguish between cyber-attacks and faults in power electronic systems such as Inverter-Based Resources (IBRs) or microgrids. This method only requires locally measured voltage and frequency as input and can distinguish these anomalies within 5 ms. The [62] study, employs a bilateral-information-based cyber-attack identification method for Cyber-Physical Power Systems (CPPSs). They utilized an Extreme Learning Machine (ELM) due to its rapid learning speed and strong generalization performance.

5. Conclusion

The use of solid state electronics to control and convert electric power is a subject that has been addressed in the field of power electronics. The important role of power electronics in various industries is undeniable. In these industries, anomalies may occur due to various factors such as voltage fluctuations, electromagnetic interference, defects in electronic components or improper operation of control systems. Therefore, there are different methods for detecting abnormalities. This survey provided an analysis of the current state of anomaly detection in power electronics using machine learning and deep learning methods.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Z. Khashroum, H. Rahimighazvini, and M. Bahrami, "Applications of Machine Learning in Power Electronics: A Specialization on Convolutional Neural Networks," ENG Transactions, vol. 4, 11/21 2023.

[2] M. Bahrami and Z. Khashroum, "Review of Machine Learning Techniques for Power Electronics Control and Optimization," arXiv preprint arXiv:2310.04699, 2023.

[3] E. H. Bayoumi, "Power electronics in renewable energy smart grid: a review," International Journal of Industrial Electronics and Drives, vol. 2, no. 1, pp. 43-61, 2015.

[4] J. He, Q. Yang, and Z. Wang, "On-line fault diagnosis and fault-tolerant operation of modular multilevel converters—A comprehensive review," CES Transactions on Electrical Machines and Systems, vol. 4, no. 4, pp. 360-372, 2020.

[5] S. Wu et al., "Unsupervised Anomaly Detection and Diagnosis in Power Electronic Networks: Informative Leverage and Multivariate Functional Clustering Approaches," IEEE Transactions on Smart Grid, 2023.

[6] A. Huang and J. Baliga, FREEDM System: Role of Power Electronics and Power Semiconductors in Developing an Energy Internet. 2009, pp. 9-12.

[7] P. Schneider and F. Xhafa, "Chapter 3 - Anomaly detection: Concepts and methods," in Anomaly Detection and Complex Event Processing over IoT Data Streams, P. Schneider and F. Xhafa Eds.: Academic Press, 2022, pp. 49-66.

[8] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review," Sensors, vol. 23, no. 8, p. 4117, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/8/4117.

[9] R. Kaur and D. Gabrijelčič, Behavior segmentation of electricity consumption patterns: A cluster analytical approach," Knowledge-Based Systems, vol. 251, p. 109236, 2022/09/05/ 2022, doi: https://doi.org/10.1016/j.knosys.2022.109236.

[10] M. Baker, A. Y. Fard, H. Althuwaini, and M. B. Shadmand, "Real-Time AI-Based Anomaly Detection and Classification in Power Electronics Dominated Grids," IEEE Journal of Emerging and Selected Topics in Industrial Electronics, vol. 4, no. 2, pp. 549-559, 2022.

[11] T. Lu, L. Wang, and X. Zhao, "Review of Anomaly Detection Algorithms for Data Streams," Applied Sciences, vol. 13, no. 10, p. 6353, 2023. [Online]. Available: https://www.mdpi.com/2076-3417/13/10/6353.

[12] A. Beattie et al., "A Robust and Explainable Data-Driven Anomaly Detection Approach For Power Electronics," in 2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), 25-28 Oct. 2022 2022, pp. 296-301, doi: 10.1109/SmartGridComm52983.2022.9961002.

[13] K. Bhatnagar, S. Sahoo, F. Iov, and F. Blaabjerg, Physics Guided Data-Driven Characterization of Anomalies in Power Electronic Systems. 2021, pp. 01-06.

[14] S. Trilles, S. S. Hammad, and D. Iskandaryan, "Anomaly detection based on Artificial Intelligence of Things: A Systematic Literature Mapping," Internet of Things, vol. 25, p. 101063, 2024/04/01/ 2024, doi: https://doi.org/10.1016/j.iot.2024.101063.

[15] M. Thwaini, "Anomaly Detection in Network Traffic using Machine Learning for Early Threat Detection," Data and Metadata, vol. 1, p. 34, 12/23 2022, doi: 10.56294/dm202272.

[16] R. K. Ray, "Exploring Machine Learning Techniques for Fraud Detection in Financial Transactions," 10/17 2023.

[17] N. Kolokas, T. Vafeiadis, D. Ioannidis, and D. Tzovaras, Forecasting faults of industrial equipment using machine learning classifiers. 2018.

[18] S. Daniel and S. Joseph, "Using Machine Learning to Monitor Equipment Health in Predictive Maintenance," 07/15 2023.

[19] P. I. Gómez, M. E. L. Gajardo, N. Mijatovic, and T. Dragičević, "A Self-Commissioning Edge Computing Method for Data-Driven Anomaly Detection in Power Electronic Systems," IEEE Transactions on Industrial Electronics, 2024.

[20] S. Sørbø and M. Ruocco, "Navigating the metric maze: a taxonomy of evaluation metrics for anomaly detection in time series," Data Mining and Knowledge Discovery, 2023/11/18 2023, doi: 10.1007/s10618-023-00988-8.

[21] A. B. Nassif, M. A. Talib, Q. Nasir, and F. M. Dakalbab, "Machine Learning for Anomaly Detection: A Systematic Review," IEEE Access, vol. 9, pp. 78658-78700, 2021, doi: 10.1109/ACCESS.2021.3083060.

[22] Zeyad Khashroum, Ali Dehghan Chaharabi, Lorena Palmero, Keiichiro Yasukawa, " Establishment and placement of a Multi-purpose Phasor measurement unit to improve parallel state estimation in distribution Networks ". 2021, Engineering Science & Technology Journal Vol. 3 No. 1, pp. 1-17.

[23] R. Foorthuis, On the Nature and Types of Anomalies: A Review of Deviations in Data. 2021.

[24] K.-H. Lai, D. Zha, J. Xu, Y. Zhao, G. Wang, and X. Hu, "Revisiting time series outlier detection: Definitions and benchmarks," in Thirty-fifth conference on neural information processing systems datasets and benchmarks track (round 1), 2021.

[25] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM computing surveys (CSUR), vol. 41, no. 3, pp. 1-58, 2009.

[26] N. Nguyen Thi, V. L. Cao, and N.-A. Le-Khac, "One-class collective anomaly detection based on LSTM-RNNs," Transactions on Large-Scale Data-and Knowledge-Centered Systems XXXVI: Special Issue on Data and Security Engineering, pp. 73-85, 2017.

[27] L. Feng et al., "Anomaly detection for electricity consumption in cloud computing: framework, methods, applications, and challenges," EURASIP Journal on Wireless Communications and Networking, vol. 2020, no. 1, p. 194, 2020/10/07 2020, doi: 10.1186/s13638-020-01807-0.

[28] L. Lei, B. Wu, X. Fang, L. Chen, H. Wu, and W. Liu, "A dynamic anomaly detection method of building energy consumption based on data mining technology," Energy, vol. 263, p. 125575, 2023/01/15/ 2023, doi: https://doi.org/10.1016/j.energy.2022.125575.

[29] A. W. Werth, "Towards distinguishing between cyber-attacks and faults in cyber-physical systems," 2014.

[30] K. Gupta, S. Sahoo, R. Mohanty, B. K. Panigrahi, and F. Blaabjerg, "Distinguishing Between Cyber Attacks and Faults in Power Electronic Systems—A Noninvasive Approach," IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 11, no. 2, pp. 1578-1588, 2022.

[31] S. K. H. Shah, A. Hellany, M. Nagrial, and J. Rizk, "Influence of environmental changes on power quality disturbances in Hybrid Renewable Energy System," Energy Reports, vol. 9, pp. 164-173, 2023/10/01/ 2023, doi: https://doi.org/10.1016/j.egyr.2023.08.047.

[32] K. H. Rao, G. Srinivas, A. Damodhar, and M. V. Krishna, "Implementation of anomaly detection technique using machine learning algorithms," International journal of computer science and telecommunications, vol. 2, no. 3, pp. 25-31, 2011.

[33] S. Asefi, M. Mitrovic, D. Ćetenović, V. Levi, E. Gryazina, and V. Terzija, "Power system anomaly detection and classification utilizing WLS-EKF state estimation and machine learning," arXiv preprint arXiv:2209.12629, 2022.

[34] L. Guo, J. Zhang, J. Ye, S. J. Coshatt, and W. Song, "Data-driven cyber-attack detection for pv farms via time-frequency domain features," IEEE transactions on smart grid, vol. 13, no. 2, pp. 1582-1597, 2021.

[35] S. Perera and S. Elphick, "Chapter 4 - Impact and management of power system harmonics," in Applied Power Quality, S. Perera and S. Elphick Eds.: Elsevier, 2023, pp. 71-130.

[36] M. I. Radaideh, C. Pappas, and S. Cousineau, "Real electronic signal data from particle accelerator power systems for machine learning anomaly detection," Data in Brief, vol. 43, p. 108473, 2022/08/01/ 2022, doi: https://doi.org/10.1016/j.dib.2022.108473.

[37] K. Kea, Y. Han, and T.-K. Kim, "Enhancing anomaly detection in distributed power systems using autoencoder-based federated learning," Plos one, vol. 18, no. 8, p. e0290337, 2023.

[38] K. A. Alaghbari, H.-S. Lim, M. H. M. Saad, and Y. S. Yong, "Deep Autoencoder-Based Integrated Model for Anomaly Detection and Efficient Feature Extraction in IoT Networks," IoT, vol. 4, no. 3, pp. 345-365, 2023. [Online]. Available: https://www.mdpi.com/2624-831X/4/3/16.

[39] S. Ahmad, K. Styp-Rekowski, S. Nedelkoski, and O. Kao, "Autoencoder-based condition monitoring and anomaly detection method for rotating machines," in 2020 IEEE International Conference on Big Data (Big Data), 2020: IEEE, pp. 4093-4102.

[40] Mohammad Aryanfar, Ghazal Rahmani-Sane, Milad Hadizadeh Masali, Ali Mosallanejad " Application of recovery techniques to enhance the resilience of power systems," Future Modern Distribution Networks Resilience, 2024/1/1, 2024, p. 195-213.

[41] A. Zadehgol-Mohammadi, M. Hosseinzadehtaher, and M. B. Shadmand, "Deep Learning-Based Real-time Anomaly Detection for Power Electronics-Dominated Grid," in 2023 IEEE Power and Energy Conference at Illinois (PECI), 2023: IEEE, pp. 1-5.

[42] M. I. Radaideh et al., "Time series anomaly detection in power electronics signals with recurrent and ConvLSTM autoencoders," Digit. Signal Process., vol. 130, no. C, p. 14, 2022, doi: 10.1016/j.dsp.2022.103704.

[43] A. Takiddin, M. Ismail, U. Zafar, and E. Serpedin, "Deep autoencoder-based anomaly detection of electricity theft cyberattacks in smart grids," IEEE Systems Journal, vol. 16, no. 3, pp. 4106-4117, 2022.

[44] M. Xiao et al., "Addressing Overfitting Problem in Deep Learning-Based Solutions for Next Generation Data-Driven Networks," Wireless Communications and Mobile Computing, vol. 2021, p. 8493795, 2021/08/15 2021, doi: 10.1155/2021/8493795.

[45] J. Wang, L. Ge, G. Liu, and G. Li, "VOVU: A Method for Predicting Generalization in Deep Neural Networks," Mathematical Problems in Engineering, vol. 2021, p. 6170662, 2021/11/23 2021, doi: 10.1155/2021/6170662.

[46] J. E. Zhang, D. Wu, and B. Boulet, "Time series anomaly detection for smart grids: A survey," in 2021 IEEE Electrical Power and Energy Conference (EPEC), 2021: IEEE, pp. 125-130.

[47] L. Cui, Y. Qu, L. Gao, G. Xie, and S. Yu, "Detecting false data attacks using machine learning techniques in smart grid: A survey," Journal of Network and Computer Applications, vol. 170, p. 102808, 2020.

[48] Shirin Besati, Somasundaram Essakiappan, Madhav Manjrekar, " A New Flexible Modified Impedance Network Converter," Systems and Control, ITEC2023, Detroit, MI, USA, 2023.

[49] I. Syarif, A. Prugel-Bennett, and G. Wills, Unsupervised Clustering Approach for Network Anomaly Detection. 2012.

[50] D. Deng, "DBSCAN clustering algorithm based on density," in 2020 7th international forum on electrical engineering and automation (IFEEA), 2020: IEEE, pp. 949-953.

[51] M. Ankerst, M. M. Breunig, H.-P. Kriegel, and J. Sander, "OPTICS: Ordering points to identify the clustering structure," ACM Sigmod record, vol. 28, no. 2, pp. 49-60, 1999.

[52] M. Ali, P. Scandurra, F. Moretti, and H. H. R. Sherazi, "Anomaly Detection in Public Street Lighting Data Using Unsupervised Clustering," IEEE Transactions on Consumer Electronics, pp. 1-1, 2024, doi: 10.1109/TCE.2024.3354189.

[53] J. D. d. Guia, R. S. Concepcion, H. A. Calinao, S. C. Lauguico, E. P. Dadios, and R. R. P. Vicerra, "Application of Ensemble Learning with Mean Shift Clustering for Output Profile Classification and Anomaly Detection in Energy Production of Grid-Tied Photovoltaic System," in 2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE), 6-8 Oct. 2020 2020, pp. 286-291, doi: 10.1109/ICITEE49829.2020.9271699.

[54] T. Katayama and S. Sugimoto, Statistical Methods in Control & Signal Processing. CRC Press, 1997.

[55] H. Wang, M. Liserre, and F. Blaabjerg, "Toward Reliable Power Electronics: Challenges, Design Tools, and Opportunities," IEEE Industrial Electronics Magazine, vol. 7, no. 2, pp. 17-26, 2013, doi: 10.1109/MIE.2013.2252958.

[56] A. T. Michael, S. Kumar, S. Mathew, and M. Pecht, "Anomaly detection in electronic products," in 2008 2nd Electronics System-Integration Technology Conference, 1-4 Sept. 2008 2008, pp. 91-96, doi: 10.1109/ESTC.2008.4684330.

[57] N. J. Johannesen, M. L. Kolhe, and M. Goodwin, "Vertical Approach Anomaly Detection Using Local Outlier Factor," in Power Systems Cybersecurity: Methods, Concepts, and Best Practices, H. Haes Alhelou, N. Hatziargyriou, and Z. Y. Dong Eds. Cham: Springer International Publishing, 2023, pp. 297-310.

[58] K. Osmani, A. Haddad, T. Lemenand, B. Castanier, M. Alkhedher, and M. Ramadan, "A critical review of PV systems' faults with the relevant detection methods," Energy Nexus, vol. 12, p. 100257, 2023/12/01/ 2023, doi: https://doi.org/10.1016/j.nexus.2023.100257.

[59] J. Yu et al., "CONGO^2: Scalable Online Anomaly Detection and Localization in Power Electronics Networks," IEEE Internet of Things Journal, vol. 9, no. 15, pp. 13862-13875, 2022, doi: 10.1109/JIOT.2022.3143123.

[60] F. Li et al., "Detection and diagnosis of data integrity attacks in solar farms based on multilayer long short-term memory network," IEEE Transactions on Power Electronics, vol. 36, no. 3, pp. 2495-2498, 2020.

[61] C. Tipton IV and D. A. R. L. A. U. States, "Survey of Fault Detection and Classification in Power Conversion Electronics," 2020.

[62] Q. Wang, X. Cai, Y. Tang, and M. Ni, "Methods of cyber-attack identification for power systems based on bilateral cyber-physical information," International Journal of Electrical Power & Energy Systems, vol. 125, p. 106515, 2021/02/01/ 2021, doi: https://doi.org/10.1016/j.ijepes.2020.106515.