

AI-Driven Anomaly and Intrusion Detection in Energy Systems: Current Trends and Future Direction

Georgios Andronikidis
Sidroco Holdings Ltd
Nicosia, Cyprus
gandronikidis@sidroco.com

Charis Eleftheriadis
Sidroco Holdings Ltd
Nicosia, Cyprus
celeftheriadis@sidroco.com

Zisis Batzos
Sidroco Holdings Ltd
Nicosia, Cyprus
zbatzos@sidroco.com

Konstantinos Kyranou
Sidroco Holdings Ltd
Nicosia, Cyprus
kkyranou@sidroco.com

Nikolaos Maropoulos
University of Western Macedonia
Kozani, Greece
aff00306@uowm.gr

Gohar Sargsyan
Celesta Advice
Amsterdam, Netherlands
g.sargsyan@gmail.com

Panagiotis Radoglou Grammatikis
Dpt. of Electrical & Computer Engineering
University of Western Macedonia
Kozani, Greece
pradoglou@uowm.gr

Panagiotis Sarigiannidis
Dpt. of Electrical & Computer Engineering
University of Western Macedonia
Kozani, Greece
psarigiannidis@uowm.gr

Abstract—The growing digitalization and interconnection of energy infrastructures have improved operational efficiency but also heightened the risk of exposure to cyber threats. Traditional electrical power and energy systems encompass all infrastructure and processes for generating, transmitting, distributing, and consuming electricity. Conversely, the smart grid represents an advanced paradigm, integrating cyber-physical components to optimize efficiency, reliability, and sustainability. However, this paradigm shift renders the energy sector more susceptible to cyber threats and attacks, necessitating proactive identification and mitigation. This survey provides a comprehensive analysis of the current state of anomaly and intrusion detection systems specifically designed for the energy sector. We review recent advancements in detection methodologies, including machine learning, artificial intelligence, and hybrid techniques, highlighting their effectiveness in identifying potential threats.

Index Terms—Artificial Intelligence, Cybersecurity, Electrical Power & Energy System, Smart Grid, Intrusion Detection, Anomaly Detection

I. INTRODUCTION

The increasing integration of advanced technologies in energy systems have significantly enhanced their efficiency, reliability, and scalability. However, this advancement has also introduced complex vulnerabilities that expose these systems to a myriad of cyber threats and anomalies. The potential consequences of such breaches range from minor disruptions to catastrophic failures, highlighting the critical need for robust anomaly and intrusion detection mechanisms.

This work has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101096456.

Artificial Intelligence (AI) and Machine Learning (ML) has emerged as a pivotal tool in amplifying the security of energy systems [1], [2]. By leveraging ML algorithms, neural networks, and other AI techniques, these systems can detect and respond to anomalies and intrusions more effectively than traditional methods. AI-driven approaches offer the ability to analyze large volumes of data in real-time, identify patterns, and predict potential threats with high accuracy.

Numerous studies have explored the application of AI in anomaly detection and intrusion prevention within energy systems [3]–[5]. Recent research outcomes showcase the potential of AI demonstrating deep learning models' efficacy in identifying irregularities in power grid operations [6] and emphasizing the superiority of AI-based methods over conventional techniques for detecting cyber-attacks in smart grids (SG) [7].

The early detection of anomalies and intrusions is crucial for safeguarding critical infrastructure that serves millions of households worldwide. In 2015, Europe experienced the first massive cyber attack on a power grid, targeting Ukraine, a cyber attack known as BlackEnergy [8]. This attack left over 230,000 consumers without electricity for one to six hours. The incident was attributed to an advanced persistent threat group known as Sandworm, which operated during the Russo-Ukrainian war.

Another campaign known as Dragonfly/EnergeticBear [9] targeted Western energy companies, with most victims located in the United States and Europe, including countries such as France, Italy, and Spain. According to Symantec Enterprise,

the attackers infiltrated critical organizations, conducting espionage, and the compromising systems had the potential to cause significant damage and disrupt energy supplies.

More recently, in May 2023, Denmark experienced its most extensive cyber-related attack [10] against critical infrastructure to date. The coordinated assault targeted 22 companies within the Danish energy sector, exploiting a critical vulnerability. The attackers gained access to the companies' industrial control systems, prompting several to operate in island mode to prevent further damage. The attack demonstrated thorough preparation and precise execution, suggesting potential involvement of state actors. The rapid detection and response by SektorCERT, facilitated by their sensor network and collaboration with stakeholders, were crucial in mitigating the operational consequences.

These incidents highlight the critical need for developing systems that can effectively detect and mitigate cyber threats, thereby making them resilient to cyber-attacks. Improving the resilience of energy systems not only fortifies them against potential disruptions but also fosters greater trust among stakeholders, including utility companies, regulators, and consumers. Moreover, robust cybersecurity measures significantly increase the positive social impact by ensuring a stable and reliable energy supply, which is essential for the smooth functioning of modern society. As cyber threats evolve, investing in advanced detection and mitigation technologies becomes indispensable for safeguarding the integrity and reliability of energy systems.

This survey paper aims to provide a comprehensive overview of the state-of-the-art AI technologies employed for anomaly and intrusion detection in electrical power and energy systems (EPES) as well as SG and microgrids. The insights garnered from this survey are intended to guide researchers and practitioners in developing more secure and resilient energy systems.

The structure of this paper unfolds as follows: This section serves as an Introduction, while Section II and Section III present the state-of-the-art technologies used for anomaly detection and intrusion detection respectively. Section IV explores the challenges associated with anomaly and intrusion detection. Section V discusses the future directions in anomaly and intrusion detection, as well as incident response. Finally, Section VI consolidates key findings and outlines future research endeavors.

II. ANOMALY DETECTION

Within the domain of EPES, SG, and microgrids, anomaly detection methodologies serve as critical guardians against cyber threats. As these infrastructures undergo continuous modernization, incorporating cutting-edge technologies and interconnected systems, the necessity for robust anomaly detection mechanisms becomes increasingly pronounced. Anomalies, whether arising from malicious intrusions or operational irregularities, possess the potential to undermine the stability and functionality of energy networks, thereby jeopardizing

their reliability and operational integrity. This section elaborates on various advanced techniques and methodologies employed to detect anomalies in the energy sector, highlighting the integration of ML and time-series analysis for improved accuracy and efficiency.

Ibrahim et al. [11] discuss various ML algorithms used in its methodology, focusing on AutoEncoder Long Short-Term Memory (AE-LSTM), Isolation Forest [12], and Facebook-Prophet¹. AE-LSTM combines unsupervised AutoEncoder and LSTM, useful for handling time-series data and reducing gradient vanishing issues with its three gates: input, forget, and output. Isolation Forest is an unsupervised anomaly detection model using decision trees to identify anomalies based on their branching depth. Finally, Facebook-Prophet is a time-series forecasting algorithm that decomposes time series data into trend, seasonal, and holiday components, extending the functionality of Twitter's Anomaly Detection². This study found that AE-LSTM effectively detects anomalies and identifies the health signal, in contrast to Facebook-Prophet and Isolation Forest.

Another study conducted by Wang et al. [13] involves an unsupervised approach that integrates closely with a load forecasting component. The technique uses forecasting results to identify anomalies in electrical load data assessing whether changes in load at the current time step align with historical load changes captured in the training set. More specifically, the anomaly detection process calculates the first-order differences in the time series data of the training dataset. These differences are used to define a range of acceptable load changes. If the load change observed at the current time step falls within this range, the load is considered normal; otherwise, it is flagged as an anomaly. This method addresses the class imbalance problem often encountered in anomaly detection by eliminating the need for labelled training data and focusing on deviations from forecasted patterns.

In Radaideh et al. [14] recurrent autoencoders (RAEs), including LSTM, GRU, and ConvLSTM models, were employed to analyze the time series data. These models were trained and validated using both normal and faulty pulses. More specifically, the approach of this study involves data pre-processing followed by model training and anomaly detection. Relevant pulse data were extracted from raw waveforms to create a structured dataset. Anomalies were detected by analyzing the reconstruction errors from the RAEs, with optimal thresholds determined empirically to minimize false positives and effectively identify anomalies. The GRU model, which uses gated recurrent units, simplifies the traditional LSTM by combining the input and forget gates, thus reducing the number of parameters and making it faster to train, albeit sometimes at the cost of performance with longer sequences. The LSTM model employs long short-term memory units that maintain a cell state over time, effectively addressing the vanishing gradient problem typical of standard RNNs, and it includes three

¹<https://facebook.github.io/prophet/>

²<https://github.com/twitter/AnomalyDetection>

gates, which control the flow of information. The ConvLSTM model integrates convolutional operations within the LSTM architecture, enabling the capture of spatiotemporal features in the data by applying convolutions in both the input-to-state and state-to-state transitions, which makes it particularly suitable for complex time-series data with spatial dependencies. The results demonstrated that while all three models provided comparable performance, LSTM showed slightly better accuracy in practical applications compared to GRU and ConvLSTM.

Moreover, Takidin et al. [15] proposed in their study an anomaly detection solution based on deep autoencoders for electricity theft cyberattacks in SGs. Particularly, various autoencoder architectures are explored to augment detection performance. The simplest model, a simple autoencoder (SAE), learns benign energy consumption patterns and identifies theft by assessing deviations from these patterns. This approach uses reconstruction errors to detect anomalies, with fully connected and sequence-to-sequence structures being compared. The fully connected SAE employs dense hidden layers for encoding and decoding, while the sequence-to-sequence SAE utilizes LSTM layers to capture temporal correlations in the data. Additionally, variational autoencoders (VAEs) and autoencoders with attention (AEA) are investigated. VAEs introduce a probabilistic element, improving detection by modeling data variability, while AEAs leverage attention mechanisms to further optimize performance. The AEAs, particularly those with sequence-to-sequence structures, show significant improvements in detection rates and false alarm rates compared to other models, due to their ability to model long sequences and complex data patterns efficiently.

A three-part approach aiming to refine the quality of wind turbine SCADA data for anomaly detection has also been explored [16]. Initially, it addresses the treatment of missing data by categorizing it into three types: Missing Completely at Random (MCAR), Missing at Random (MAR), and Missing Not at Random (MNAR). The methodology proposes handling each type appropriately to avoid introducing bias. Following this, the study introduces explicit and obvious anomaly filtering to remove data instances indicating faults or curtailments based on specific SCADA features such as blade pitch and power reference values. The approach is divided into three strategies: Unfiltered, Filtered, and Split, each with distinct impacts on data handling and subsequent anomaly detection. Lastly, the methodology evaluates five anomaly detection techniques — including Isolation Forest, Gaussian Mixture Models (GMM), Local Outlier Factor (LOF), and KNN — on their effectiveness in cleaning the wind turbine power curve while maintaining the statistical variability of the wind speed feature.

III. INTRUSION DETECTION

Intrusion detection in EPES, SG, and microgrids is a critical aspect of guaranteeing the security and resilience of modern energy infrastructures. With the increasing integration of digital technologies and the intense interconnection, these systems are becoming more vulnerable to cyber attacks, posing

significant threats to their reliability and safe operation. As such, there is a growing need for effective intrusion detection mechanisms tailored specifically to the unique characteristics and requirements of EPES, SG, and microgrids.

This section explores various state-of-the-art approaches for intrusion detection in these energy systems, aiming to provide insights into the diverse methodologies and techniques employed to safeguard against cyber threats. Panthi et al. [17] proposed a Binary Grey Wolf Optimization-based Ensemble Classification (BGWO-EC) framework designed to classify events as normal or attack. This framework consists of four distinct phases: pre-processing, feature selection, classification, and evaluation. Initially, the pre-processing phase involves replacing infinite values with zero. Next, the BGWO metaheuristic method is applied for feature selection, followed by feeding these features into various classification algorithms to train the model. The supervised models are repeatedly trained using a 10-fold cross-validation setup, while the hyperparameters of the models are fine-tuned using the Bayesian optimization technique to ensure their robustness and efficiency.

Another work focuses on developing an intrusion detection system based on the DNP3 [18] protocol which is heavily used in EPES. To address the challenge of making reliable decisions under uncertainty, the Inter-Domain Evidence-theoretic Approach for Inference (IDEA-I) [19] is proposed. This approach reframes the detection problem by utilizing Dempster–Shafer (DS) [20] theory to reduce false alerts. IDEA-I employs a multi-hypothesis mass function model, which integrates probability scores from supervised-learning classifiers. A location-cum-domain-based fusion framework then evaluates the detector’s performance using disjunctive, conjunctive, and cautious conjunctive rules. The framework processes sensor data from various sources, including substation networking devices and SCADA systems. Pre-processed data is synchronized using a Mean Value-Based Time Synchronization block, and mass functions are computed based on DS combination rules. This process culminates in a decision function that is further refined using NSGA-2 based feature selection. By addressing the uncertainty and variability in intrusion detection system (IDS) outputs, IDEA-I enhances situational awareness in cyber-physical systems.

The proposed solution in [21] involves developing an intrusion detection method tailored for power industrial control systems using a hyperparameter-optimized Random Forest (RF) classifier. This method includes several key steps: First, the original dataset is preprocessed and split into training and validation sets using 5-fold cross-validation. Next, a hyperparameter configuration space is created, and RF classifiers are built with various hyperparameter combinations, followed by training and testing. A RF regression model is then constructed to evaluate the importance of each hyperparameter using functional ANOVA [25]. Subsequently, an improved grid search algorithm (IGSA) optimizes each hyperparameter sequentially based on its importance. The optimized hyperparameters are used to build the best RF classifier, validated on the test set, demonstrating superior performance in terms of accuracy,

TABLE I: This table summarizes the latest Anomaly Detection and Intrusion Detection methodologies.

Studies	Methodology	Task	AI Algorithm	Outcome
Ibrahim et al. [11]	Anomaly Detection	Classification or Regression	AE-LSTM Isolation Forest Facebook-Prophet	AE-LSTM detects anomalies and identifies health signal
Wang et al. [13]		Regression	GRU Bi-LSTM TDG	Eliminates class imbalance problem occurred in anomaly detection
Radaideh et al. [14]		Regression	GRU LSTM ConvLSTM	LSTM demonstrated better performance
Takidin et al. [15]			SAE VAE AEA	AEA demonstrates significant improvement in detection rates
Morisson et al. [16]		Classification	Isolation Forest GMM KNN LOF	Various algorithms are evaluated with the proposed pre-processing step
Panthi et al. [17]	Intrusion Detection	Classification	Decision Tree KNN Optimizable Ensemble SVM	The BGWO-EC boost the performance of the detectors
Sahu et al. [19]		Classification	Decision Tree KNN SVM Random Forest	Addresses uncertainty and variability in intrusion detection
Zhu et al. [21]		Classification	Random Forest	A hyperparameter configuration space is constructed, and used to build various Random Forest classifiers
Wang et al. [22]		Classification	Decision Tree KNN AdaBoost Bagging	By using the proposed dimensionality reduction (SupervisedAE and PCA), models demonstrate superior accuracy and F1 score
Roy et al. [23]		Classification	Decision Tree KNN AdaBoost CDEL Logistic Regression Naïve Bayes	CDEL algorithm demonstrates better performance over traditional classifiers
Durairaj et al. [24]		Classification	EDBN	EDBN demonstrates higher accuracy and lower false alarm rates

precision, recall, F1 score, and roc_auc score compared to traditional grid search and other classifiers.

Traditional IDS approaches often struggle with high-dimensional data, leading to overfitting and suboptimal performance. To address this, Wang et al. [22] introduces a dimensionality reduction technique combining a supervised autoencoder (SupervisedAE) and principal components analysis (PCA) [26]. The SupervisedAE integrates label information during training, optimizing both reconstruction and classification errors to generate more discriminative latent representations. This step is followed by applying PCA to further reduce feature dimensions, ensuring more efficient and effective data processing. The model's performance was validated using a public power system dataset, where it demonstrated superior accuracy and F1 scores compared to other dimension reduction methods and existing IDS techniques. The proposed IDS framework involves preprocessing data with min-max normalization, training the SupervisedAE for initial dimension reduction, applying PCA for further reduction, and finally using the processed data to train various classifiers.

The Cluster-Driven Ensemble Learning (CDEL) algorithm proposed in [23] is capable of detecting cyberattacks in Automatic Generation Control Systems (AGCS) by combining the strengths of K-means clustering and multiple Support

Vector Machines (SVMs). By clustering the data and using ensemble methods, CDEL effectively addresses overlapping patterns and complex attack scenarios, ensuring robust and accurate classification. This approach demonstrates superior performance over traditional classifiers and maintains high predictive accuracy even in noisy environments.

Finally, the Enhanced Deep Belief Network (EDBN) approach, proposed in [24] for intrusion detection in microgrids combines deep learning with rule-based techniques to improve the detection accuracy of cyberattacks. This method integrates multiple layers of network components, control systems, and application interfaces to create a comprehensive security architecture. By employing a layered microgrid architecture and incorporating user-defined rules, EDBN effectively identifies and mitigates False Data Injection (FDIA) and Denial of Service (DoS) attacks. The experimental results demonstrate that the EDBN technique achieves higher accuracy rates and lower false alarm rates compared to existing methods, making it a robust solution for maintaining the stability and security of microgrid operations. Additionally, the integration of user-defined rules enhances the detection process by dynamically updating based on the microgrid's behavior, further increasing the system's resilience against sophisticated cyber threats.

Table I presents a summary of recent methodologies pro-

posed by researchers for anomaly and intrusion detection. In the subsequent section will delve into the challenges identified in this sector.

IV. CHALLENGES

The study of anomaly detection and intrusion detection systems reveals numerous challenges, ranging from the complexity of identifying sophisticated threats to the limitations of current technologies in distinguishing between benign and malicious activities. One critical challenge is the detection of zero-day and complex attacks at both the software and hardware levels without any prior knowledge. As highlighted by [27], there is a pressing need for advanced detection approaches capable of identifying these sophisticated threats in real time, underscoring the importance of evolving current methodologies to address these emerging challenges.

Furthermore, research by [28] identifies several other significant challenges faced by anomaly and intrusion detection systems. These include high false alarm rates, low detection rates, unbalanced datasets, and slow response times. These issues impede the effectiveness of detection systems, as false alarms can lead to resource wastage, and low detection rates may allow threats to go unnoticed. Additionally, unbalanced datasets can skew the performance of detection algorithms, while slow response times can hinder timely threat mitigation, intensify the potential impact of intrusions.

Additionally, the robustness of ML and AI-based detectors against adversarial attacks is a crucial concern. As noted by recent studies [29], these systems must be fortified to withstand such attacks, ensuring their reliability and effectiveness in real-world applications. Addressing these adversarial threats requires ongoing research and development to improve the robustness of detection systems, ultimately leading to more secure and reliable anomaly and intrusion detection mechanisms.

Finally, ensuring compatibility and interoperability with legacy systems, enabling seamless integration of advanced cybersecurity measures, is mandatory. On top of that, addressing regulatory and compliance issues is critical, as evolving standards and policies will shape the implementation of these technologies. Harmonizing new solutions with existing frameworks will be essential for widespread adoption and maintaining regulatory compliance across diverse jurisdictions.

V. FUTURE DIRECTIONS

To address the identified challenges in anomaly and intrusion detection systems, future research and development must leverage state-of-the-art technologies to create more effective and resilient solutions. One promising direction is the integration of large language models (LLMs) and advanced ML algorithms. These models can be trained on vast datasets in order to upgrade their understanding and identification of complex attack patterns. By utilizing LLMs, detection systems can assist security experts in understanding the attack patterns and procedures used by the malicious users. Similarly, LLMs can be used in order to provide mitigation actions.

Another future direction involves the development of more sophisticated adversarial training techniques to fortify ML and AI-based detectors against adversarial attacks [30]. Enriching the training process of these ML-based systems with adversarial examples can improve their robustness, making it more difficult for attackers to exploit weaknesses. Additionally, the implementation of transfer learning can allow models trained on one type of data to be effectively applied to different, yet related, datasets. This approach can help in overcoming the challenge of unbalanced datasets, enabling the models to generalize better across various scenarios.

Federated learning technologies present a significant advancement in the field of anomaly and intrusion detection systems, offering a collaborative approach to amplifying detection capabilities without compromising data privacy. By enabling multiple organizations to train a shared ML model on their local data, federated learning allows the collective optimization of detection algorithms without the need to exchange sensitive information. This approach addresses the challenge of unbalanced datasets by pooling diverse data sources, leading to more comprehensive and generalized models that can detect a wider range of anomalies and intrusions. Moreover, federated learning elevates data security by keeping raw data localized, thereby reducing the risk of data breaches. The decentralized nature of this technology also makes it more resilient to targeted attacks, as there is no central point of failure. As federated learning continues to evolve, its application in anomaly and intrusion detection systems promises to significantly bolster their effectiveness and robustness, facilitating a more collaborative and secure cybersecurity landscape.

Finally, future directions should consider the cyber-physical security challenges arising from the integration of information technology and operational technology. Proactive cyber-defense strategies are essential, along with fostering Human-AI collaboration and incorporating human-in-the-loop practices to upgrade system security and adaptability.

VI. CONCLUSION

This study presents a comprehensive overview of the current trends and future directions in AI-driven anomaly and intrusion detection systems within the energy sector. With the increasing digitalization and interconnectedness of energy infrastructure, the risk of cyber threats has significantly risen. This research highlights the effectiveness of ML, statistical approaches, and hybrid techniques in identifying potential threats and mitigating risks before they would escalate. The integration of AI technologies, such as deep learning models, autoencoders, and ensemble learning frameworks, has demonstrated superior performance over traditional methods in detecting anomalies and intrusions.

Key findings include the importance of early detection mechanisms in safeguarding critical infrastructure, as evidenced by past cyber attacks like BlackEnergy, Dragonfly/EnergeticBear, and the recent coordinated assault on the Danish energy sector. This study also emphasizes the necessity of

developing robust and proactive defense strategies tailored to the unique characteristics of EPES, SG, and microgrids.

The future of anomaly and intrusion detection lies in the strategic incorporation of cutting-edge AI and ML technologies, coupled with domain-specific enhancements for the energy sector. These innovations promise to overcome the current limitations, providing more accurate, secure, and resilient detection systems capable of addressing the evolving landscape of cyber threats. Continued research and interdisciplinary collaboration will be crucial in realizing these advancements, ultimately leading to more robust and reliable security infrastructures.

In conclusion, the integration of AI and ML in anomaly and intrusion detection represents a promising direction for the energy sector. Continued advancements and proactive defense strategies will be essential in protecting critical infrastructure and maintaining operational integrity in the face of increasingly sophisticated cyber threats.

ACKNOWLEDGMENT

This work has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101096456.

REFERENCES

- [1] P. R. Grammatikis, P. Sarigiannidis, E. Iturbe, E. Rios, A. Sarigiannidis, O. Nikolis, D. Ioannidis, V. Machamint, M. Tzifas, A. Giannakoulis *et al.*, "Secure and private smart grid: The spear architecture," in *2020 6th IEEE Conference on Network Softwarization (NetSoft)*. IEEE, 2020, pp. 450–456.
- [2] V. Kelli, P. Radoglou-Grammatikis, A. Sesis, T. Lagkas, E. Fountoukidis, E. Kafetzakis, I. Giannoulakis, and P. Sarigiannidis, "Attacking and defending dnp3 ics/scada systems," in *2022 18th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. IEEE, 2022, pp. 183–190.
- [3] I. Siniosoglou, P. Radoglou-Grammatikis, G. Efstathopoulos, P. Fouliras, and P. Sarigiannidis, "A unified deep learning anomaly detection and classification approach for smart grid environments," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1137–1151, 2021.
- [4] X. Wang and S.-H. Ahn, "Real-time prediction and anomaly detection of electrical load in a residential community," *Applied Energy*, vol. 259, p. 114145, 2020.
- [5] Y. Himeur, K. Ghanem, A. Alsalemi, F. Bensaali, and A. Amira, "Artificial intelligence based anomaly detection of energy consumption in buildings: A review, current trends and new perspectives," *Applied Energy*, vol. 287, p. 116601, 2021.
- [6] Y. Luo, Y. Xiao, L. Cheng, G. Peng, and D. Yao, "Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities," *ACM Computing Surveys (CSUR)*, vol. 54, no. 5, pp. 1–36, 2021.
- [7] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *Journal of Big Data*, vol. 7, no. 1, p. 41, Jul 2020. [Online]. Available: <https://doi.org/10.1186/s40537-020-00318-5>
- [8] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, no. 1-29, p. 3, 2016.
- [9] F. B. Khan, A. Asad, H. Durad, S. M. Mohsin, and S. N. Kazmi, "Dragonfly cyber threats: A case study of malware attacks targeting power grids," *Journal of Computing & Biomedical Informatics*, vol. 4, no. 02, pp. 172–185, 2023.
- [10] SectorCert, "The attack against danish, critical infrastructure," 2023.
- [11] M. Ibrahim, A. Alsheikh, F. M. Awaysheh, and M. D. Alshehri, "Machine learning schemes for anomaly detection in solar power plants," *Energies*, vol. 15, no. 3, 2022. [Online]. Available: <https://www.mdpi.com/1996-1073/15/3/1082>
- [12] 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.
- [13] X. Wang, Z. Yao, and M. Papaefthymiou, "A real-time electrical load forecasting and unsupervised anomaly detection framework," *Applied Energy*, vol. 330, p. 120279, 2023. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0306261922015367>
- [14] M. I. Radaideh, C. Pappas, J. Walden, D. Lu, L. Vidyaratne, T. Britton, K. Rajput, M. Schram, and S. Cousineau, "Time series anomaly detection in power electronics signals with recurrent and convlstm autoencoders," *Digital Signal Processing*, vol. 130, p. 103704, 2022. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1051200422003219>
- [15] 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.
- [16] R. Morrison, X. Liu, and Z. Lin, "Anomaly detection in wind turbine scada data for power curve cleaning," *Renewable Energy*, vol. 184, pp. 473–486, 2022. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0960148121017134>
- [17] M. Panthi and T. Kanti Das, "Intelligent intrusion detection scheme for smart power-grid using optimized ensemble learning on selected features," *International Journal of Critical Infrastructure Protection*, vol. 39, p. 100567, 2022. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1874548222000518>
- [18] G. Clarke, D. Reynnders, and E. Wright, *Practical modern SCADA protocols: DNP3, 60870.5 and related systems*. Newnes, 2004.
- [19] A. Sahu and K. Davis, "Inter-domain fusion for enhanced intrusion detection in power systems: An evidence theoretic and meta-heuristic approach," *Sensors*, vol. 22, no. 6, 2022. [Online]. Available: <https://www.mdpi.com/1424-8220/22/6/2100>
- [20] G. Shafer, "Dempster-shafer theory," *Encyclopedia of artificial intelligence*, vol. 1, pp. 330–331, 1992.
- [21] N. Zhu, C. Zhu, L. Zhou, Y. Zhu, and X. Zhang, "Optimization of the random forest hyperparameters for power industrial control systems intrusion detection using an improved grid search algorithm," *Applied Sciences*, vol. 12, no. 20, 2022. [Online]. Available: <https://www.mdpi.com/2076-3417/12/20/10456>
- [22] C. Wang, H. Liu, Y. Sun, Y. Wei, K. Wang, and B. Wang, "Dimension reduction technique based on supervised autoencoder for intrusion detection of industrial control systems," *Secur. Commun. Netw.*, vol. 2022, pp. 1–12, Jun. 2022.
- [23] S. D. Roy, S. Debbarma, and A. Iqbal, "A decentralized intrusion detection system for security of generation control," *IEEE Internet of Things Journal*, vol. 9, no. 19, pp. 18924–18933, 2022.
- [24] D. Durairaj, T. K. Venkatasamy, S. U. Abolfazl Mehbodniya, and T. Alam, "Intrusion detection and mitigation of attacks in microgrid using enhanced deep belief network," *Energy Sources, Part A: Recovery, Utilization, and Environmental Effects*, vol. 46, no. 1, pp. 1519–1541, 2024. [Online]. Available: <https://doi.org/10.1080/15567036.2021.2023237>
- [25] F. Hutter, H. Hoos, and K. Leyton-Brown, "An efficient approach for assessing hyperparameter importance," in *International conference on machine learning*. PMLR, 2014, pp. 754–762.
- [26] J. Shlens, "A tutorial on principal component analysis," 2014.
- [27] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, p. 20, Jul 2019. [Online]. Available: <https://doi.org/10.1186/s42400-019-0038-7>
- [28] M. Al-Janabi, M. A. Ismail, and A. H. Ali, "Intrusion detection systems, issues, challenges, and needs," *Int. J. Comput. Intell. Syst.*, vol. 14, no. 1, pp. 560–571, 2021.
- [29] D. Han, Z. Wang, Y. Zhong, W. Chen, J. Yang, S. Lu, X. Shi, and X. Yin, "Evaluating and improving adversarial robustness of machine learning-based network intrusion detectors," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 8, pp. 2632–2647, 2021.
- [30] C. Eleftheriadis, A. Symeonidis, and P. Katsaros, "Adversarial robustness improvement for deep neural networks," *Machine Vision and Applications*, vol. 35, no. 3, p. 35, 2024. [Online]. Available: <https://doi.org/10.1007/s00138-024-01519-1>