Journal of Engineering and Technology for Industrial Applications

ITEGAM-JETIA

Manaus, v.12 n.58, p 963-969. March/April, 2026.
DOI: https://doi.org/10.5935/jetia.v12i58.3219

ISSN ONLINE: 2447-0228

RESEARCH ARTICLE OPEN ACCESS

A REVIEW ON AI BASED FAULT AND ANOMALY DETECTION IN POWER SYSTEMS

Jenisha K J[1] and Rajeswari R[2]

[1]Assistant Professor (CF), Department of Electrical and Electronics Engineering, Government College of Technology, Coimbatore, Tamil Nadu, India.
[2]Professor, Department of Electrical and Electronics Engineering, Government College of Technology, Coimbatore, Tamil Nadu, India.

[1]http://orcid.org/0009-0000-7997-6898, [2]https://orcid.org/0000-0002-2585-493X

Email: jenisha.eee@gct.ac.in, rreee@gct.ac.in

ARTICLE INFO

Article History
Received: January 02, 2026
Reviewed: February 03, 2026
Accepted: March 10, 2026
Published: April 30, 2026

Keywords:
Artificial intelligence,
Deep learning,
Anomaly monitoring
Cyber security

ABSTRACT

Power systems are becoming more complex because of large-scale integration of renewable energy, the widespread generation of electricity from various sources, electric vehicle charging networks, advanced power electronic converters, and significant automation through digital substations and smart grid technologies. These changes create new operational conditions with less system inertia, two-way power flows, and highly variable generation patterns. This leads to non-linear, rapidly changing, and data-heavy disturbances that are hard to detect and isolate using traditional relay-based protection methods. Conventional protection systems, which rely on preset thresholds, fixed setups, and basic network models, often have trouble with high levels of inverter-based resources, layout changes, and communication delays. In this context, artificial intelligence offers strong data-driven methods that can learn complex system behavior directly from data. It can uncover hidden traits, identify types and locations of faults, spot early and developing anomalies, and assist with smart, adaptable decision-making almost in real time. This review outlines key AI techniques, including machine learning, deep learning, fuzzy logic, and reinforcement learning. It examines how recent studies have used these methods for fault detection, diagnosis, classification, and anomaly monitoring in transmission, distribution, and microgrid environments. Additionally, this paper addresses practical issues such as data quality, limited labels, class imbalance, model generalization across different network setups, computational demands, and constraints for real-time use in digital relays and edge devices.

I. INTRODUCTION

Contemporary society relies on power systems that function safely, dependably, and consistently to sustain essential infrastructure, industry, transport, and communication services. Contemporary power systems face numerous disruptions such as equipment wear and tear, insulation breakdown, faults in lines and cables, unusual and fluctuating load conditions, switching and protective actions, sporadic renewable energy generation, failures of power-electronic converters, and more frequent cyber incidents. If faults and abnormal conditions go undetected or are recognized too late, they can lead to cascading failures, widespread blackouts, faster equipment deterioration, safety risks, and significant reliability and financial losses.

Traditional protection strategies predominantly depend on established thresholds, preset relay configurations, and simplified system hypotheses, which may fail to adequately reflect the highly dynamic, nonlinear, and data-driven characteristics of modern smart grids, marked by inverter-based resources, two-way power flows, and regular network reconfigurations. Moreover, conventional techniques frequently exhibit restricted sensitivity to emerging faults, sporadic anomalies, and slight variations in operational patterns, particularly in the presence of noisy data and communication lags.

Artificial intelligence offers robust data-driven instruments that can detect intricate patterns, learn system behavior from extensive measurement data, adjust to evolving operational conditions, and pinpoint early warning signals that may not be readily apparent via traditional analytical methods. This review outlines essential AI methods for detecting faults and anomalies in power systems, provides a summary of recent advancements in applications related to transmission, distribution, and microgrids, and addresses practical challenges in deployment like data accessibility and labeling, class imbalance, interpretability of models, constraints in real-time implementation, compatibility with existing protection systems, and resilience against measurement uncertainties and cyber-physical threats. Additionally, the document emphasizes new prospects for future advancement, such as adaptive and self-refreshing protection strategies, hybrid models that combine physics-informed and data-driven approaches, explainable and reliable AI for operator trust, and resilient frameworks that improve the reliability and security of next-generation intelligent protection systems.

II. LITERATURE REVIEW

By [1] developed a dynamic risk assessment model for cyber-physical power systems under cyber-attacks, emphasizing the integration of cyber vulnerabilities and physical consequences. The methodology involved assessing network security vulnerabilities in SCADA systems with substations, considering existing software vulnerabilities and defines mechanisms, corrected by propagation characteristics. Physical consequences were evaluated through minimum load shedding under N-I Consistency scenarios. According to [2] developed an intelligent fault diagnosis method for lithium-ion batteries in electric vehicles, focusing on timely fault state detection and degree identification. The method applied support vector machine to classify the symptom of fault, the discrete cosine method to remove the noise , and introduced the modified covariance Matrix to reduce effects of current variation of condition indicators. Grid search was used in order to optimize the SVM parameters. The test result showed that MCM-based model had good accuracy and timeliness, proved the feasibility of proposed method for future fault management strategies.

In turn [3] aimed to detect fraudulent behavior and malfunctions in smart meter data using a hybrid ML approach. The approach included using unsupervised ML on smart meter time series data to discover anomalous values. Spectral Residual-Convolutional Neural Network (SR-CNN) and a martingale-based anomaly detector were applied to data.. Based on the separated asymmetrical data, the two classes boosted decision tree and fisher linear discriminant analysis were utilized for classification. By [4] investigated to enhance the security of smart grid SCADA systems by developing a novel AI based framework to detect and prevent network intrusions. The methodology involved the preprocessing and normalization of benchmark datasets, applications of Zaira Ebola search optimization(ZESO) algorithm to achieve the feature extraction , and association of Deep Random Kernal Forest Classification (DRKFC)organized at the reliable attack detection procedure.

In turn [5] discusses both traditional and deep learning methods for anomaly detection and fault location in power grid datasets. The paper explains how deep networks (e.g., DNN,CNN,RNN) are employed to extract deep features from time-series grid data and improve detection and localization accuracy compared to conventional approaches. It also highlights challenges like data noise, spatiotemporal feature extraction, and the robustness of AI models in grid operations. According to [6] categorizes AI application in to fault data processing, modeling, and hyper parameter optimization (HPO). It demonstrate how AI technique such as GANs address class imbalance, how deep learning improves decision accuracy and how hybrid model can achieve near perfect detection accuracy . It also discusses optimization methods like evolutionary algorithms for enhancing AI performance .

By [7] provide a concise but informative overview of how artificial intelligence technique and transforming fault detection and diagnosis in power systems , with particular emphasize on distribution network where most faults occur. The authors explain the conventional protection and monitoring approaches , although reliable under well-defined operating condition, struggle when the grid becomes complex,variable,and saturated with distributed energy resources. Nature scientific report constructs an AI framework that merges cyber and physical grid data for anomaly detection using LSTM network and random forests for classification with very high accuracy. It also uses explainable AI for interpretability and adversarial training for robustness against attacks such as False data injection and DoS attacks [8].

Khan and colleagues examine AI based fault detection framework across transmission and distribution systems and compare them with classical techniques. Their study categorizes AI approaches into supervised learning, unsupervised learning and deep learning, providing examples of how each is applied in practice. Deep learning architecture such as CNNs and LSTMs are shown to capture nonlinear and time dependent fault behavior more effectively than traditional approaches. They conclude that future systems will likely integrate physics-based model with AI to improve accuracy, reliability and trustworthiness [9]. According to [10] suggested to enhance the reliability, safety, and security of smart hybrid renewable-based micro grids by developing novel control strategies for fault diagnosis and cyber -attack resilience. The methodology was based on design on fault tolerant control using optimal fuzzy gain-scheduling technique to counteract power loss faults and attack resilient control utilizing estimated sensor values fasting data integrity attacks.

III. RESEARCH CHALLENGES AND LIMITATIONS

Even with significant progress in AI- driven faults detection and cyber-physical security for modern power systems, many critical research challenges and practical limitations remain. These issues must be addressed before widespread implementation can take place. A major problem is that many cyber-physical risk evaluation and security analysis framework still rely on overly simplify threat assumptions, specific attack paths, and limited attacker capabilities. These modelling methods cannot fully capture the complex interactions between the dynamics of physical power networks and cyber communication systems. As a results, they struggle to represent coordinated, multi-phase, and adaptive cyber-physical attacks in real operational environments. Furthermore, most of the case studies are conducted on small or medium test setups, and validation with actual utility-scale infrastructure is rare, which greatly undermines trust in their relevance to larger interconnected networks [1], [20].

A significant limitation is the heavy dependence of data-driven fault diagnosis and intrusion detection methods on large, high-quality labelled datasets. Machine learning models, such as support vector machines, convolutional neural networks, and hybrid CNN-RNN architecture, require well-representative training data to perform consistently however, actual power system datasets are often very imbalanced, with normal operating conditions dominating and fault or attack incidents occurring infrequently, and inconsistent labelling across substations and utilities. These challenges severely hinder the models' learning abilities and can lead to biased decision boundaries and poor detection performance in new situations [2], [5], [6], [23].

While data augmentation techniques and generative models like GANs have aim to address data scarcity and imbalance, these methods add further complexity to both model design and training. The quality of samples generated synthetically relies heavily on careful architecture selection and hyper parameter tuning. . Poor tuning can lead to unrealistic fault patterns that harm classifier performance on real data. Additionally, methods for feature selection and model tuning that depend on optimization increase computational demands. This complicates their use in real-time protection and monitoring systems that have strict latency requirements [5], [16].This problem become even more significant for wide-area monitoring and protection applications that rely on high-resolution synchro phasor data and fast decision-making.

The interpretability and transparency of AI models are still major challenges for safety-critical power systems. Deep learning models often function as black boxes, providing little insight in to the reasons behind specific alarms, classification results, or control decisions. For protection engineers and system operators it is crucial to understand why a relay acted or why an anomaly triggered an alert. This knowledge is vital for maintaining system safety and avoiding unnecessary tripping or cascading failures. This lack of transparency make it essential to accept deep learning-based protection systems, especially in important areas like transmission line protection, generator safeguarding, and cyber-attack prevention methods [8], [12], [21].

New decentralized learning and security systems, such as federated learning and blockchain architectures, provide promising solutions for protecting privacy, enabling collaborative learning, and resisting data manipulation. However, implementing them in large energy systems comes with many ongoing challenges. Regular model updates and distributed consensus processes canlead to significant communication overhead. This result in high network traffic and great risk of communication failures. Additionally, latency and synchronization issues between control centers and substations in different areas can lower real-time performance. Scalability is a major concern because of the increasing number of participating nodes and data sources in today's smart grid environments. Making sure that distributed learning agents while meeting real-time operational constraints continues to be a tough research problem [13], [14], [19], [22].

From a methodological perspective, traditional statistical methods and control chart techniques struggle to adapt in rapidly changing operational conditions. These methods usually assume stable processes and clear statistical features. However this rarely happens in today's power systems, which are marked by variable renewable generation, flexible loads, and frequent topology changes. Their effectiveness dropped significantly during short production runs and rapidly changing conditions, where there is not enough historical data to accurately estimate statistical parameters accurately [11]. On the other hand, advanced AI-driven models, can adapt more easily but often overfit when trained on limited or specific data. Overfitted models may perform very well in controlled environments but have trouble when faced with unexpected disturbances, new protection parameters, or unfamiliar network setups [3], [25].

High-impedance fault detection is a long-standing challenge. These faults produce weak and very inconsistent signatures, which load fluctuations, switching transients, and background noise can easily hide. Monitoring wind turbines and renewable energy converters is also tough due to non-stationary operational characteristics, mechanical-electrical interactions, and environmental factors like temperature and wind speed. Classifying power quality events is getting more complicated as distributed energy resources, power electronic converters, and electric vehicle charging systems introduce new disturbance patterns and harmonic interactions. Current feature extraction and learning models often had a hard time staying reliable amid rapidly changing grid dynamics and significant renewable integration [17], [18], [24].

A major limitation is that most current studies primarily focus on detection and classification accuracy as the main performance metric. However, effective power system operation requires not only accurate detection but also synchronized and quick response plans. There is limited research on how outputs from AI-based detection can interact with adaptive protection settings, corrective action strategies, or wide-area control systems. The lack of closed-loop systems that manage detection, decision-making, and control at the same time limit the real-world effectiveness of many proposed approaches. Additionally, the connection between AI-based decision support systems and traditional protection devices, such as distance relays, differential relays, and overcurrent relays, is rarely explored in depth [4], [7], [9], [10].

Integrating AI models into current grid systems present significant implementation challenges. Older protection and supervisory control systems were not build to handle data-heavy learning algorithms or frequent model updates. Limited computing resources at substations, strict certification requirements for protection systems, and careful operational practices make adoption difficult. Additionally compatibility issues among various vendors, data formats, and communication protocols make large-scale implementation difficult. Without standard interfaces and validation methods, ensuring consistent performance across different platforms. Cyber-physical co-simulation environments and digital twins have been proposed to improve the testing and validation of advanced security and protection systems.

However, creating high-fidelity models that accurately represent both cyber infrastructures and the dynamics of physical power systems remains a complex task. Streamlining communication models, security logic, and human operator actions can lead to overly optimistic assessments of system robustness. Furthermore, maintaining and updating digital twins is necessary to reflect changing network configurations and operational methods, which increases development costs and complexity [1], [20]. Ultimately, future smart grids need hybrid and scalable systems that combine the benefits of physics-driven models, statistical approaches, and advanced machine learning techniques. Data-driven solutions rely heavily on data quality, concept drift, and vulnerabilities to adversarial manipulation, while model-based approaches struggle to capture the complex nonlinear dynamics and cyber interactions.

Therefore, there is an urgent need for resilient, understandable, and flexible hybrid architectures that incorporate system knowledge, security concepts, and network constraints into learning frameworks. These integrated solutions should enable adaptive protection, coordinated cyber-physical responses, and seamless integration with existing operational infrastructures to ensure the secure and reliable functioning of future power systems [4], [7], [9], [10].For Reference, Comparison Summary of AI based Anomaly detection techniques in Power systems is provided in Table 1 below.

Table1: Comparative Analysis of AI based anomaly detection in power systems.

Study /Author	Main Focus	Method / AI Used	Key Contribution
Yan et al.	Cyber-physical risk	Cyber + load-shedding modeling	Links cyber-attacks to physical grid impacts
Yao et al.	EV battery faults	SVM + noise reduction	Accurate, timely battery fault diagnosis
Oprea et al.	Smart meter anomalies	SR-CNN + hybrid classifiers	Fraud + malfunction detection
Rabie et al.	SCADA intrusion	Feature optimization + deep forest	High-accuracy cyber-attack detection
Sun et al.	Grid anomaly & fault location	CNN/RNN/DNN	Improved spatiotemporal detection
Liu et al.	Data imbalance & HPO	GANs + optimization	Near-perfect classification with tuning
Nazim et al.	Distribution faults	Review & analysis	AI better than conventional protection
Nature report	Cyber-physical AI	LSTM + RF + explainable AI	Robust and interpretable framework
Khan et al.	Transmission + distribution	Comparative AI review	Demonstrates advantage of deep learning
Jadidi et al.	Micro grid resilience	Fault-tolerant + attack-resilient control	Maintains stability under faults and cyber attacks
Meira et al.	Process deviation detection	Statistical control charts	Shows limitations of classical anomaly detection in short production runs
Guo et al.	Protection relay anomalies	KPCA + Isolation Forest	Detects abnormal relay behavior in distribution networks
Anand et al.	Secure data storage	Bio-inspired optimization	Improves data security and privacy in cloud-based smart grids
Yamany et al.	IoT cyber resilience	Federated learning + swarm optimization	Enhances cyber-attack resilience without centralized data
Hou et al.[15]	AI parameter optimization	Improved Grey Wolf Optimization	Achieves faster convergence and improved tuning performance
Hu et al.	Wind power forecasting	Improved Deep Belief Network	Accurate forecasting under nonlinear and uncertain conditions
Liu et al.	Wind turbine blade faults	Deep learning + cloud-edge framework	Enables scalable and real-time damage detection
Veerasamy et al.	High-impedance fault detection	LSTM-RNN	Reliable detection of hard-to-identify faults in PV systems
Hasan et al.	Smart grid cyber security	Blockchain + big data analytics	Secures energy trading and data integrity
Tatipatri & Arun	Cyber-attacks in power systems	Review & taxonomy	Comprehensive classification of cyber-attacks and detection methods
Yusifov & Muradli	Relay protection limitations	Analytical study	Identifies weaknesses of conventional relay protection schemes
Li et al.	False data injection attacks	Federated learning	Privacy-preserving detection of cyber-attacks
Nassif et al.	Anomaly detection techniques	Systematic ML review	Consolidates ML-based anomaly detection methods
Rodrigues et al.	Power quality events	Deep learning (CNN-based)	Accurate classification of power quality disturbances
Qu et al.	Energy consumption anomalies	Genetic algorithm + AdaBoost	Optimized ensemble learning for anomaly detection

Source: Authors, (2026).

IV. CONCLUSION

The reviewed literature shows that artificial intelligence is a strong tool for fault detection, anomaly monitoring and cyber resilience in modern power systems. This includes diagnosing problems at the component level, such as lithium-ion battery failures in electric vehicles and issues with converters and sensors. It also covers risk assessments, intrusion detection, and situational awareness in SCADA and energy management systems. Unlike traditional rule-based and signal-processing protection methods, AI techniques perform better in handling non-linear dynamics, complex data, and rapidly changing operational conditions. Deep learning models like convolutional neural networks (CNNs), recurrent neural networks (RNNs), and long short-term memory (LSTM) networks helps extract complex spatial and temporal relationships from synchro phasors, smart meter, and substation data. Standard analysis struggles to capture, especially during periods of high renewable energy integration and low system inertia. Furthermore hybrid learning models that combine unsupervised anomaly detection with supervised fault classification significantly improve detection accuracy and sensitivity to early faults.

They also provide better resilience against noise, missing data, and class imbalance. AI-powered optimization techniques, transfer learning, GAN-based data augmentation, and improved feature learning enhance model performance across different networks designs and scenarios. The growing connection between cyber security and the reliability of power systems is clear in the literature. Cyber-attacks, like false data injection, replay attacks, and coordinated intrusion strategies, can leads to serious physical consequences. These includes improper relay operations and decreased stability overall stability. Research shows that AI-driven systems improve detection speed, accuracy, and flexibility. They also support predictive and preventive measures, help operator's decisions and encourage strong, intelligence, and self-correcting power system operations. Also, emerging trends shows the need for explainable AI, physics-based learning, and edge-based deployment. These elements are vital for reliable, scalable, and real-time implementation of AI-powered protection and monitoring systems in future smart grids.

V. AUTHOR'S CONTRIBUTION

Conceptualization: Rajeswari.R
Methodology: Jenisha K J
Investigation: Rajeswari.R , Jenisha K J
Discussion of results:. Rajeswari.R , Jenisha K J
Writing – Original Draft: Jenisha K J
Writing – Review and Editing: Rajeswari.R
Resources: Jenisha K J
Supervision: Rajeswari.R
Approval of the final text: Rajeswari.R

VI. ACKNOWLEDGMENTS

The authors sincerely thank Government College of Technology (GCT) for allowing access to advanced research facilities through the Research Centre of Excellence – Alternate Energy Research Laboratory. The Centre's laboratory facilities, technical support, and research environment greatly helped with the literature review, analysis, and critical assessment of recent advancements in AI-driven fault and anomaly detection in power systems. The authors appreciate the valuable academic discussions and help from the faculty members and researchers at GCT, which improved the technical quality, clarity, and organization of this review paper. The support and resources from the Research Centre of Excellence – Alternate Energy Research Laboratory were crucial for the successful completion of this review study.

VII. FUTURE SCOPE

Although, AI based methods shows promise, several important research areas till need attention before we can use them widely in real power system protection and monitoring, First, there is a strong need for real-time, scalable, and deployable AI systems that can operate reliably under rapidly changing load patterns, high uncertainity in renewable generation, increasing integration of inverter-based resources, and evolving cyber threats. Most current studies rely on offline simulations, lab tests, or publicity available benchmark datasets , which do not fully capture the practical challenges . Therfore, future research should focus on extensive field trails and utility grade implementations that consider realistic communication delays, data synchronization errors, packet losses, missing and corrupted measurements, varying sensor quality, and limitations of intelligent electronic devices(IEDs) digital relays, and edge-computing platforms.In addition, we need model compression, lightweight designs, and hardware-aware AI to ensure that advanced learning models can meet the strict latency and relaiablity need of protection applications.

Second, we should develop hybrid protection and monitoring frameworks that merge data-driven AI models with physics-based system models, power system dynamics, and traditional protection logic. This improvement will enhance model clarity , operational stability and operator confidence. Purely data-driven solution often lack physical consistency and may make decisions under new operating conditions, changes in topology, or rare Extreme events. Techniques like physics-informed learning, digital twin-assisted training, and co-simulation of protection and control systems can improve generalization and reduce on large labelled datasets. Additionally, explainable AI (XAI) techniques are difficult for understanding the internal process of complex models. This understanding helps protection engineers and system operators know why a specific fault classification, islanding decision, load – shedding command, or cyber-attack isolation action was taken. Such clarity is vital for compliance with regulations acceptance by operators, post-event analysis and safe collaboration between humans and machines in future control centers.

Third ,AI based monitoring and protection systems encounter challenges from sensor issues, measurement noise, model drift, and international data tampering. Adversarial attacks, data poisoning , replay attacks, and false data injection can mislead learning models, which might lead to incorrect relay operations, delayed fault isolation, or control actions. Future research should focus on secure learning methods, anomaly-aware training, adversarial and trust-aware decision- making across diverse data sources. Integrating cyber security analytics in to protection and monitoring processes will be vital for detecting coordinated cyber-physical attacks. This ensure that protection decisions stay reliable, even if communication and sensing systems are compromised.

Fourth, the absence of standardized, large-scale, and openly accessible datasets still makes it hard to benchmark and replicate research fairly. Most current datasets comes from specific test systems, simulation tools, and attack scenerios which complicate how Algorithms are compared. Creating standardized open datasets that encompass various operating conditions, fault types, levels of renewable integration, cyber-attack scenarios, and communication behaviors- while maintaining data privacy and utility confidentiality- will speed up methodological progress and objective evaluation of AI algorithms. Furthermore, we need to establish commom evaluation metrics, testing protocols, and validation frameworks to support clear and consistent performance assessments across different research efforts.

Fifth, future research should focus on continuous learning, online adaptation, and transfer learning techniques to handle changing system setups, seasonal load variations, equipment aging, and fluctuating market and operational conditions. AI models in real electric grids must be able to update themselves without needing frequent offline retraining or complete redeployment. Federated and distributed learning approaches can help multiple utilities to work together on modern development while keeping data private and reducing communication needs. These methods are especially attracted for large interconnected power systems and widely distributed microgrids.

Finally, future power systems will gain a lot from fully integrated cyber-physical monitoring and protection systems . These system will bring together fault and anomaly detection, cybersecurity analytics, predictive maintenance, stability assessment, and fault-tolerant control within one operational framework. A close integration of AI-driven situational awareness with wide-area measurement systems, digital substations, and energy management systems will help support proactive and coordinated decision-making across generation, transmission, and distribution levels. These systems can give early warnings of cascading failures, smart self-healing actions, coordinated protection setting, and resilient recovery strategies after major disturbances or cyber incidents. In the end, these improvement will create next generation smart grids and microgrids that are not only intelligent, but also secure, flexible, understanding , and highly reliable. This will ensure a sustainable and trustworthy operation of future power infrastructure

VIII. REFERENCES

[1] Yan et al. (2022) – "A cyber-physical power system risk assessment model against cyber-attacks." Published in: IEEE Systems Journal, 17(2), 2018–2028.

[2]. Yao et al. (2021) – "An intelligent fault diagnosis method for lithium battery systems based on grid search support vector machine." Published in: Energy, 214, 118866.

[3] Oprea et al. (2021) – "Anomaly detection with machine learning algorithms and big data in electricity consumption." Published in: Sustainability, 13(19), 10963.

[4] El Ghaly (2025) – "Hybrid ML Algorithm for Fault Classification in Transmission Lines Using Multi-Target Ensemble Classifier with Limited Data." Published in: Eng, 6(1), 4.

[5] Lin et al. (2022) – "Short-term load forecasting based on LSTM networks considering attention mechanism." Published in: Int. J. of Electrical Power & Energy Systems, 137, 107818.

[6] Bakkar et al. (2022) – "Artificial intelligence-based protection for smart grids." Published in: Energies, 15(13), 4933.

[7] Rabie et al. (2022) – "A proficient ZESO-DRKFC model for smart grid SCADA security." Published in: Electronics, 11(24), 4144.

[8] Ahmad et al. (2021) – "A bio-inspired heuristic algorithm for solving optimal power flow problem in hybrid power system." Published in: IEEE Access, 9, 159809–159826.

[9] Estebsari et al. (2021) – "IoT-enabled real-time management of smart grids with demand response aggregators." Published in: IEEE Transactions on Industry Applications, 58(1), 102–112.

[10] Jadidi et al. (2023) – "Active fault-tolerant and attack-resilient control for a renewable microgrid against power-loss faults and data integrity attacks." Published in: IEEE Transactions on Cybernetics, 54(4), 2113–2128.

[11] Meira et al. (2022) – "Analysis of deviation from nominal control chart performance on short production runs." Published in: Production, 32, e20210092. https://doi.org/10.1590/0103-6513.20210092

[12] Guo et al. (2022) – "Anomaly detection method for protection relay system in distribution networks based on KPCA-IF model." Published in: Proc. CICED 2022, IEEE, pp. 1590–1595. https://doi.org/10.1109/CICED56215.2022.9929202

[13] Anand et al. (2022) – "Enhanced bacterial foraging optimization algorithm for secure data storage and privacy-preserving in cloud." Published in: Peer-to-Peer Networking and Applications, 15(4), 2007–2020. https://doi.org/10.1007/s12083-022-01322-7

[14] Yamany et al. (2023) – "Swarm Optimization-Based Federated Learning for the Cyber Resilience of IoT Systems." Published in: IEEE Transactionson Consumer Electronics, 70(1), 1359–1369. https://ui.adsabs.harvard.edu/link_gateway/2024ITCE...70.1359Y/doi:10.1109/TCE.2023.3319039

[15] Hou et al. (2022) – "Improved grey wolf optimization algorithm and application." Published in: Sensors, 22(10), 3810.

[16] Hu et al. (2021) – "Improved DBN-based hybrid forecasting method for wind power." Published in: Energy, 224, 120185.

[17] Liu et al. (2022) – "Cloud-edge-end cooperative detection of wind turbine blade damage using deep learning." Published in: IEEE Internet Computing, 27(1), 43–51.

[18] Veerasamy et al. (2021) – "LSTM recurrent neural network classifier for high impedance fault detection in solar PV systems." Published in: IEEE Access, 9, 32672–32687.

[19] Hasan et al. (2022) – "Blockchain tech on smart grid, energy trading, and big data: security issues." Published in: Wireless Communications and Mobile Computing, 2022, 9065768.

[20] Tatipatri & Arun (2024) – "Review on cyber-attacks in power systems: Detection and cyber security." Published in: IEEE Access, 12, 18147–18167.

[21] Yusifov & Muradli (2023) – "Limitation of modes with relay protection." Published in: Proc. 1st Int. Conf. on 4th Industrial Revolution & IT, Baku.

[22] Li et al. (2022) – "Detection of false data injection attacks in smart grid via federated learning." Published in: IEEE Transactions on Smart Grid, 13(6), 4862–4872.

[23] Nassif et al. (2021) – "Machine learning for anomaly detection: A systematic review." Published in: IEEE Access, 9, 78658–78700.

[24] Rodrigues et al. (2023) – "Deep learning for power quality event detection using grid data." Published in: IEEE Transactions on Instrumentation and Measurement, 72, 1–11.

[25] Qu et al. (2021) – "Genetic optimization with AdaBoost for anomaly detection in energy use." Published in: Energy and Buildings, 248, 111193.