AI Based Fault and Anomaly Detection in Power Systems

JENISHA K J[1], DR. R. SURESH KUMAR[2]
[1]*Assistant Professor (CF), Department of Electrical and Electronics Engineering, Government College of Technology, Coimbatore, Tamil Nadu, India.*
[2]*Assistant Professor, Department of Electrical and Electronics Engineering, Anna University Regional Campus, Coimbatore, Tamil Nadu, India.*

Abstract- ***Artificial -based infiltration system detection systems (IDs) are emerging as an important defense mechanism for modern power systems, which are rapidly weak for cyber-attacks due to comprehensive digitization, integration of IOT devices and dependence on comprehensive field communication networks. Traditional rules-based IDS methods often fail to detect sophisticated hazards such as false data injection attacks, refusal-service (DOS), and load-transport infiltration, especially large scale, smart grids were distributed. The AI-operated IDS leverage machine learning, deep learning, and hybrid models to detect discrepancy, adapted to develop the attack pattern, and supported real-time status awareness. This review examines the approach to detect state-of-the-art AI-based infiltration for electrical systems, which focus on detection methods, datasets, evaluation matrix and implementation challenges. Special emphasis is given to explain capacity, scalability and integration with supervisory control and data acquisition (SCADA), Phasor Measurement Units (PMU), and distributed energy resources (DERS). Finally, open research intervals and future instructions are highlighted, including federated learning, graphs in graph neural network-based detections include graph neural network-based detections and digital twin-capable cyber-flexibility.***

Keywords: Infiltration detection system (IDS), Artificial Intelligence, Fals Data Injection Attack, Cyber-Figure Security, Power System Protection.

I. INTRODCTION

The growing digitalization and automation of power systems have changed traditional grids into interconnected cyber-physical smart grids. While these developments allow for efficient monitoring, control, and integration of renewable energy sources, they also make critical infrastructure vulnerable to various cyber security threats. Attacks like false data injection (FDI), denial-of-service (DoS), malware intrusions, and load-altering attacks can undermine the reliability, stability, and security of modern power systems, potentially causing blackouts and economic losses. Intrusion Detection Systems (IDS) have become essential for improving grid cyber security. Traditional IDS methods, mainly based on signature matching and set rules, struggle to identify new and evolving threats. Additionally, the massive amount and speed of data created by Supervisory Control and Data Acquisition (SCADA) systems, Phasor Measurement Units (PMUs), and Internet of Things (IoT) devices require smart, scalable, and flexible detection systems. Artificial Intelligence (AI) offers potential solutions to these issues. By using machine learning, deep learning, reinforcement learning, and hybrid intelligent systems, AI-based IDS can recognize complex patterns, spot anomalies in real time, and adjust to new attack methods. These systems can also link cyber and physical measurements, enhancing situational awareness across wide-area networks.

This review aims to provide an overview of AI-based intrusion detection techniques in power systems. It examines current methods, application areas, datasets, and ways to measure performance. The paper also brings attention to key challenges like interpretability, scalability, data privacy, and resilience against attacks. Finally, it discusses future research directions, focusing on explainable AI, federated learning, digital twin-enabled cyber security, and graph-based intrusion detection designed for power grid structures.

II. LITERATURE REVIEW

Yan et al., [1] developed a dynamic risk assessment model for cyber-physical power systems (CPPS) under cyberattacks, emphasizing the integration of cyber vulnerabilities and physical consequences. The methodology involved assessing network security vulnerabilities in SCADA systems within substations, considering existing software vulnerabilities and defines mechanisms, corrected by

propagation characteristics. Physical consequences were evaluated through minimum load shedding under N-1 contingency scenarios. Simulations were conducted on modified IEEE 14-bus and 118-bus systems. The findings demonstrated the model's effectiveness, highlighting the critical role of cyber vulnerabilities in CPPS and the necessity of incorporating both cyber and physical aspects in risk assessment.

Yao et al., [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 (SVM) to classify the symptoms of faults, the discrete cosine filtering methods (DCFM) to remove the noise, and introduced the modified Covariance Matrix (MCM) to reduce the effects of current variation of condition indicators. Grid search was used in order to optimize the SVM parameters. The test results showed that MCM-based model had good accuracy and timeliness, proved the feasibility of proposed method for future fault management strategies.

Oprea et al., [3] aimed to detect fraudulent behaviour 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-Class Boosted Decision Tree and Fisher Linear Discriminant analysis were utilized for classification. The outcome found that the model had 90% accuracy, precision of 0.875, and F-1 score of 0.894, providing high level of effectiveness in detection of abusive consumption.

El Ghaly., [4] utilized to enhance fault detection and classification in transmission lines using efficient ML techniques, especially under constraints of limited training data. Conventional algorithms were first tested on dataset of 7681 examples and their high accuracy level was the result of the symmetry of work with electrical signals. To assess practical relevance the dataset has been cut down to 231 training samples. A new Multi-Target Ensemble Classifier was then designed which proved better than the comparison models like KNN, SVC, random forest and others. The proposed method got an overall accuracy of 0.829165, shows that the proposed method play a good role in improving fault classification in power system.

Lin et al., [5] suggested to enhance short-term zonal electricity load forecasting by developing a dual-stage attention-based LSTM network capable of generating probabilistic forecasts. The method was based on a two-stage attention mechanism: Feature attention-based encoder for feature selection from input features and temporal attention-based decoder to model temporal dependencies. Only the outputs with these characteristics were combined using a univariate LSTM trained with the pinball loss function for probabilistic forecasting. The idea was based on the GEFCom2014 dataset and compared against the other models showing higher accuracy and generalization and discovering its ability to support feature and weather station selection for the load forecast.

Bakkar et al., [6] developed and validate an adaptive protection strategy for Microgrids (MGs) integrated into smart grids, addressing the limitations of conventional methods. The method is based on the comparison between traditional protection techniques (overcurrent and differential relays) with an ANN-based protection technique. The ANN approach provided the communication abilities among protective devices and was equipped with backup mechanism aboard the same line. Simulations by MATLAB was carried out and experiments on simulated smart grid were performed. Results indicated that the AI-based protection has higher adaptation, accuracy and response time to discard the relay setting adjustment that manually can performed in the grid reconfiguration situation or DG injection level variation.

Rabie et al., [7] 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, application of Zaire Ebola search optimization (ZESO) algorithm to achieve the feature extraction, and association of Deep Random Kernel Forest Classification (DRKFC) organized at the reliable attack detection procedure. Due to the applicability of the limitations of the former models, the Meta-Heuristic–Driven approach was designed to improve the previous model's complexity, speed,

precision. And the introduced ZESO-DRKFC framework, got high detection accuracy of 99%, superior performance across multiple evaluation metrics ahead other methods.

Ahmad et al., [8] aimed to solve the Optimal Power Flow (OPF) problem in hybrid power systems incorporating thermal, wind, and solar sources by developing a bio-inspired Bird Swarm Algorithm (BSA). The methodology consisted of formulating the non-linear and non-convex OPF problem that takes into account, uncertainties of load demand and stochastic outputs from renewable power sources. Tests have been done on modified IEEE-30 bus test system. An analysis was performed on efficiency of BSA with other evolutionary metaheuristic algorithms. The study results indicated that BSA was able to obtain more accurate and stable solutions in which two case studies have the minimum generation cost of $863.121/h, $890.728/h verified its advantage.

Estebsari et al., [9] developed a real-time management schema for distribution networks experiencing volatility due to distributed renewable sources and emerging loads like electric vehicles. The approach employed Internet of Things (IoT) technologies to enable the interworking for operators of the system, and for the aggregators to foster, ancillary services including power balancing, and voltage regulation. Two algorithms have been proposed one based on Modified Optimal Power Flow to solve power balance and other based on Voltage Sensitivity Matrix for voltage control. Real-time simulation tested built from real-residential networks data prove the schema's validity to be in the efficient management of changing emphatic grid incidence.

Jadidi et al., [10] suggested to enhance the reliability, safety, and security of smart hybrid renewable-based microgrids by developing novel control strategies for fault diagnosis and cyber-attack resilience. The methodology was based on design of fault-tolerant control (FTC) using optimal fuzzy gain-scheduling technique to counteract PV power loss faults and attack resilient control (ARC) utilising estimated sensor values facing data integrity attacks. Both FTC and ARC presented an integrated intrusion detection and fault diagnosis (IDFD) system based on fuzzy model. Simulations in MATLAB/Simulink with an advanced microgrid benchmark proved the offered strategies to yield stable and safe microgrid operation.

III. ANALYSIS AND DISCUSSION

The review studies explain the role of Artificial Intelligence in improving fault detection, anomaly detection, and data intrusion in power systems. Each study addresses specific areas, from cyber-physical attacks to battery fault diagnosis and microgrid resilience. However, they show common trends, strengths, limitations, and research gaps that can guide future efforts. From these ten studies, we can observe major research trends.

Hybridization of AI techniques: The trend toward combining multiple AI algorithms, such as hybrid ML in [3] and optimization-enhanced IDS in [7], arises from the need to balance accuracy, flexibility, and generalizability.

Shift toward real-time and adaptive systems: ANN-based adaptive protection in [6] and IoT-enabled management in [9] highlight the push for responsive, autonomous systems that can adjust to changing conditions.

Cyber-physical integration and resilience: From Yan et al.'s cyber-physical risk assessment in [1] to Jadidi et al.'s integrated intrusion detection and fault tolerance in [10], the field recognizes the need to address both cyber and physical aspects to ensure resilience.

CONCLUSION

Future research in AI-based fault and intrusion detection for power systems should focus on solutions that are accurate, explainable, scalable, and practical to implement. One important direction is to develop explainable AI (XAI) frameworks to improve transparency and trust in critical decision-making. This is especially important in protection and intrusion detection, where black-box models pose challenges. Another key trend is adopting federated learning and privacy-preserving approaches, allowing collaborative training across utilities and distributed energy resources without sharing sensitive raw data. To ensure effectiveness in real-time settings, researchers must emphasize lightweight and edge-deployable AI models that can run efficiently on limited-resource devices within

microgrids and IoT-based infrastructures. Additionally, using digital twins offers a new way for continuous monitoring, predictive anomaly detection, and proactive system resilience. Lastly, the strength of AI systems against adversarial attacks and data poisoning is a critical research gap that needs future methods capable of resisting intentional manipulations while maintaining system reliability and security.

REFERENCES

[1] Hasan, M. K., Alkhalifah, A., Islam, S., Babiker, N. B., Habib, A. A., Aman, A. H. M., & Hossain, M. A. (2022). Blockchain technology on smart grid, energy trading, and big data: security issues, challenges, and recommendations. Wireless Communications and Mobile Computing, 2022(1), 9065768.

[2] Tatipatri, N., & Arun, S. L. (2024). A comprehensive review on cyber-attacks in power systems: Impact analysis, detection, and cyber security. IEEE Access, 12, 18147-18167.

[3] Yusifov, S., & Muradli, M. (2023, May). Limitation of modes with relay protection. In 1st INTERNATIONAL CONFERENCE ON THE 4th INDUSTRIAL REVOLUTION AND INFORMATION TECHNOLOGY (Vol. 1, No. 1, pp. 291-295). Azərbaycan Dövlət Neft və Sənaye Universiteti.

[4] Li, Y., Wei, X., Li, Y., Dong, Z., & Shahidehpour, M. (2022). Detection of false data injection attacks in smart grid: A secure federated deep learning approach. IEEE Transactions on Smart Grid, 13(6), 4862-4872.

[5] Nassif, A. B., Talib, M. A., Nasir, Q., & Dakalbab, F. M. (2021). Machine learning for anomaly detection: A systematic review. Ieee Access, 9, 78658-78700.

[6] Rodrigues, N. M., Janeiro, F. M., & Ramos, P. M. (2023). Deep learning for power quality event detection and classification based on measured grid data. IEEE Transactions on Instrumentation and Measurement, 72, 1-11.

[7] Qu, Z., Liu, H., Wang, Z., Xu, J., Zhang, P., & Zeng, H. (2021). A combined genetic optimization with AdaBoost ensemble model for anomaly detection in buildings electricity consumption. Energy and Buildings, 248, 111193.

[8] Chandrasekaran, K., Selvaraj, J., Xavier, F. J., & Kandasamy, P. (2021). Artificial neural network integrated with bio-inspired approach for optimal VAr management and voltage profile enhancement in grid system. Energy Sources, Part A: Recovery, Utilization, and Environmental Effects, 43(21), 2838-2859.

[9] Ilo, A., & Schultis, D. L. (2022). A holistic solution for smart grids based on LINK-paradigm (Vol. 340). Berlin/Heidelberg, Germany: Springer.

[10] Yan, K., Liu, X., Lu, Y., & Qin, F. (2022). A cyber-physical power system risk assessment model against cyberattacks. IEEE Systems Journal, 17(2), 2018-2028.