Enhancing Resilience: Smart Grid Cybersecurity and Fault Diagnosis Strategies

Abstract:

The increasing integration of advanced technologies within the power grid infrastructure has led to significant advancements in efficiency, reliability, and sustainability. However, this integration also introduces new vulnerabilities, particularly in the realm of cybersecurity. This paper presents an overview of smart grid cybersecurity challenges and proposes strategies for enhancing resilience through fault diagnosis techniques. Firstly, the paper examines the evolving threat landscape facing smart grids, encompassing cyber-attacks, insider threats, and natural disasters. It highlights the critical need for robust cybersecurity measures to safeguard grid operations and prevent potentially catastrophic disruptions. Next, the paper delves into various cybersecurity frameworks and standards tailored specifically for smart grids, emphasizing the importance of comprehensive risk assessment, intrusion detection systems, and secure communication protocols. Additionally, it discusses the role of machine learning and artificial intelligence in augmenting cyber defense capabilities, enabling proactive threat detection and rapid response. Furthermore, the paper explores fault diagnosis strategies aimed at maintaining grid resilience in the face of cyber incidents or physical faults. It discusses the integration of data analytics, predictive modeling, and real-time monitoring to identify and mitigate potential grid disturbances swiftly.

Keywords: Smart Grid, Cybersecurity, Resilience, Fault Diagnosis

1. Introduction

The integration of advanced technologies within the power grid infrastructure has revolutionized the way electricity is generated, transmitted, and distributed[1]. Smart grids, enabled by cutting-edge digital communication and control systems, promise enhanced efficiency, reliability, and sustainability[2]. However, this transformation also brings forth a new set of challenges,

particularly in the realm of cybersecurity[3]. As smart grids become increasingly interconnected and reliant on digital infrastructure, they become more vulnerable to cyber threats, including malicious attacks, insider breaches, and disruptions caused by natural disasters[4]. Ensuring the resilience of smart grids against these threats is paramount to maintaining the stability and security of the entire energy infrastructure[5, 6]. This paper explores the critical importance of enhancing resilience through smart grid cybersecurity measures and fault diagnosis strategies[7]. By examining the evolving threat landscape, discussing cybersecurity challenges specific to smart grids, and proposing proactive approaches to bolster resilience, this paper aims to provide insights into safeguarding the reliability and security of modern power grids[8]. The concept of a smart grid represents a paradigm shift in the traditional electric power system, leveraging advanced technologies to transform the way electricity is generated, transmitted, and distributed[9, 10]. Smart grid technologies encompass a wide array of innovations, including advanced metering infrastructure (AMI), distribution automation systems, energy storage, renewable energy integration, and grid-edge devices[11]. These technologies enable real-time monitoring, control, and optimization of grid operations, leading to improved efficiency, reliability, and sustainability. One of the key features of smart grids is their ability to facilitate bidirectional communication between grid components, allowing for dynamic coordination and optimization of electricity flows. This bidirectional communication enables utilities to gather detailed information about grid conditions, energy consumption patterns, and equipment performance, facilitating more informed decision-making and proactive management of grid assets[12]. Furthermore, smart grid technologies enable the integration of renewable energy sources, such as solar and wind power, into the grid infrastructure[13]. By leveraging advanced forecasting algorithms and predictive analytics, smart grids can efficiently manage the variability and intermittency inherent in renewable energy generation, thereby enhancing grid stability and resilience[14]. Additionally, smart grid technologies empower consumers to actively participate in energy management through demand response programs, time-of-use pricing, and energy-efficient technologies[15]. By providing consumers with real-time information about their energy usage and enabling them to adjust their consumption patterns accordingly, smart grids promote energy conservation and reduce peak demand, ultimately leading to cost savings and environmental benefits[16, 17]. Overall, the adoption of smart grid technologies is essential for modernizing the electric power system, enhancing grid resilience, and addressing the challenges

of the 21st century, including climate change, energy security, and the transition to a clean energy future[18]. By embracing these technologies and fostering innovation, utilities can unlock new opportunities for efficiency improvements, cost reductions, and environmental sustainability, ultimately benefiting both consumers and society as a whole[19].

1.1.Power Grid Cybersecurity: A Growing Imperative

Figure 1,the digital evolution of power grids brings unparalleled benefits, but it also introduces a myriad of challenges, particularly in the realm of cybersecurity[20]. The threat landscape is characterized by an array of adversaries ranging from financially motivated hackers to nation-state actors, each with distinct capabilities and motivations[21]. The potential consequences of a successful cyber-attack on a power grid extend beyond mere inconvenience, encompassing economic losses, societal disruption, and even threats to national security[22].

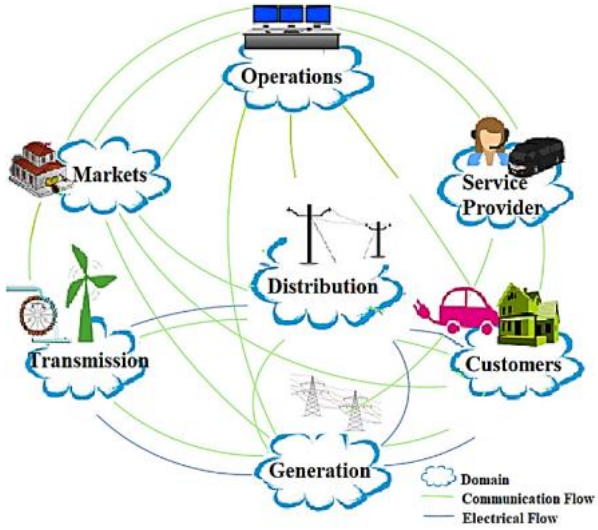

Figure 1: Power Grid Cybersecurity

As power grids increasingly embrace the concept of the Internet of Things (IoT) and interconnectivity, the attack surface expands exponentially[23]. Vulnerabilities in legacy systems, inadequately secured communication networks, and the proliferation of connected devices create a complex cybersecurity landscape[24]. The integrity of power grid operations becomes contingent on the ability to thwart cyber threats that exploit vulnerabilities in software, hardware, and the human element[25]. The incorporation of advanced cybersecurity measures becomes paramount[26]. This involves the deployment of intrusion detection systems, firewalls,

encryption protocols, and continuous monitoring to detect and respond to anomalous activities[27]. Furthermore, the development of a robust cybersecurity culture within energy organizations is crucial, emphasizing the importance of training personnel, implementing secure coding practices, and establishing incident response plans[28]. As the digital transformation of power grids unfolds, this researchserves as a beacon, guiding the industry toward a secure and adaptive future[29]. The intersection of cybersecurity and fault resilience is not merely a technological challenge; it is a holistic endeavor that requires collaboration among policymakers, industry leaders, and cybersecurity experts[30, 31]. Together, they must navigate the intricate terrain of standards, regulations, and technological innovations to forge a path that ensures the reliability and security of the power grid in an era defined by connectivity and interdependence[32]. In the ensuing sections of this research, we delve into the intricate details of power grid cybersecurity, explore dynamic fault diagnosis techniques, and present the outcomes of our methodology[33]. Through a synthesis of theory and practical implementation, we aim to contribute to the evolving discourse on safeguarding critical infrastructure in an era where the convergence of the digital and physical worlds necessitates unwavering resilience and proactive security measures[34].

The importance of resilience in maintaining grid reliability and security cannot be overstated, especially in the context of modern energy systems characterized by increasing complexity, interconnectivity, and vulnerability to disruptions[35]. Resilience refers to the ability of a system to withstand and recover from adverse events, whether they are caused by natural disasters, cyber-attacks, equipment failures, or other unforeseen circumstances[36, 37]. In the context of electric power grids, resilience plays a critical role in ensuring the uninterrupted delivery of electricity to consumers, safeguarding public safety, and protecting national security[38]. One of the primary reasons why resilience is essential for grid reliability and security is its role in mitigating the impact of disruptions and minimizing downtime[39]. By building resilient grid infrastructure and implementing proactive measures to anticipate and respond to disruptions, utilities can reduce the likelihood and duration of power outages, thereby minimizing economic losses, productivity disruptions, and societal impacts[40]. Moreover, resilience is essential for protecting critical infrastructure and ensuring the continuity of essential services, such as healthcare facilities, emergency response systems, and telecommunications networks[41, 42]. In times of crisis, such as natural disasters or cyber-attacks, these services rely on a resilient power

grid to maintain operations and support emergency response efforts, including disaster recovery and relief efforts. Furthermore, resilience enhances grid security by reducing the likelihood of successful attacks and limiting their potential impact on grid operations[43]. By implementing robust cybersecurity measures, physical security protocols, and contingency plans, utilities can mitigate the risks posed by malicious actors and minimize the potential for disruptions caused by cyber-attacks, sabotage, or other security threats. Additionally, resilience promotes innovation and adaptation in response to evolving threats and changing operating conditions[44]. By continuously monitoring grid performance, analyzing emerging risks, and implementing proactive measures to address vulnerabilities, utilities can enhance their ability to adapt to new challenges and maintain grid reliability and security in the face of uncertainty[45, 46]. By prioritizing resilience and investing in proactive measures to strengthen grid infrastructure, utilities can enhance their ability to withstand disruptions, protect critical infrastructure, and ensure the reliable delivery of electricity to consumers, even in the most challenging circumstances[47].

2. Strategies for Enhancing Smart Grid Cybersecurity

Strategies for enhancing smart grid cybersecurity are critical to safeguarding modern energy systems against evolving cyber threats[48]. These strategies encompass a range of proactive measures aimed at identifying vulnerabilities, protecting critical infrastructure, and mitigating the risks posed by malicious actors. Here are several key strategies for enhancing smart grid cybersecurity[49]. Comprehensive Risk Assessment: Conducting a thorough risk assessment is essential for identifying potential cybersecurity vulnerabilities and prioritizing mitigation efforts. This includes assessing the security posture of grid components, identifying potential attack vectors, and evaluating the potential impact of cyber threats on grid operations[50, 51]. Intrusion Detection Systems (IDS): Implementing intrusion detection systems enables utilities to monitor network traffic and detect suspicious activity in real-time[52]. IDS can help identify potential cyber-attacks, unauthorized access attempts, and anomalous behavior, allowing for timely response and mitigation[53]. Secure Communication Protocols: Utilizing secure communication protocols, such as Transport Layer Security (TLS) and IPsec, helps protect data transmitted between grid components from interception or tampering by unauthorized parties[54]. Implementing encryption and authentication mechanisms ensures the confidentiality, integrity,

and authenticity of communication channels[55, 56]. Employee Training and Awareness: Providing comprehensive cybersecurity training and awareness programs for employees, contractors, and third-party vendors is essential for promoting a culture of cybersecurity within the organization[57]. Educating personnel about common cyber threats, best practices for secure behavior, and the importance of maintaining strong security hygiene helps mitigate the risks posed by human error and insider threats[58, 59]. Network Segmentation: Implementing network segmentation divides the smart grid infrastructure into separate, isolated networks or zones, each with its security controls and access policies[60]. This limits the scope of potential cyber-attacks and reduces the risk of lateral movement by malicious actors within the network[61]. Continuous Monitoring and Threat Intelligence: Implementing continuous monitoring and threat intelligence capabilities enables utilities to detect emerging cyber threats and proactively respond to potential risks[62]. This includes monitoring network traffic, analyzing security logs, and leveraging threat intelligence feeds to stay informed about the latest cyber threats and attack trends[63].By adopting these strategies and implementing a comprehensive cybersecurity program, utilities can enhance the resilience of smart grids and mitigate the risks posed by cyber threats, safeguarding critical infrastructure and ensuring the reliable delivery of electricity to consumers[64].

2.1.Dynamic Fault Diagnosis: Safeguarding Operational Integrity

Figure 2, cybersecurity focuses on intentional threats, and dynamic fault diagnosis is concerned with fortifying the power grid against unintentional faults that can occur due to equipment failures, environmental factors, or operational errors[65]. The intricate nature of power systems, with numerous components operating in unison, demands a proactive approach to fault diagnosis to maintain operational integrity[66, 67]. Dynamic fault diagnosis techniques leverage advanced monitoring and sensor technologies to detect anomalies and deviations from normal operating conditions[68]. These techniques encompass real-time data analysis, machine learning algorithms, and predictive modeling to identify and isolate faults swiftly[69]. The objective is to prevent faults from cascading into widespread failures, ensuring the resilience of the power grid against unforeseen events. The integration of dynamic fault diagnosis with cybersecurity forms a synergistic approach to power grid resilience[70]. While cybersecurity measures protect against intentional threats, dynamic fault diagnosis fortifies the grid's ability to withstand internal faults

and disruptions[71]. This comprehensive strategy aligns with the overarching goal of ensuring the reliability and continuous operation of the power grid in the face of diverse challenges[72].

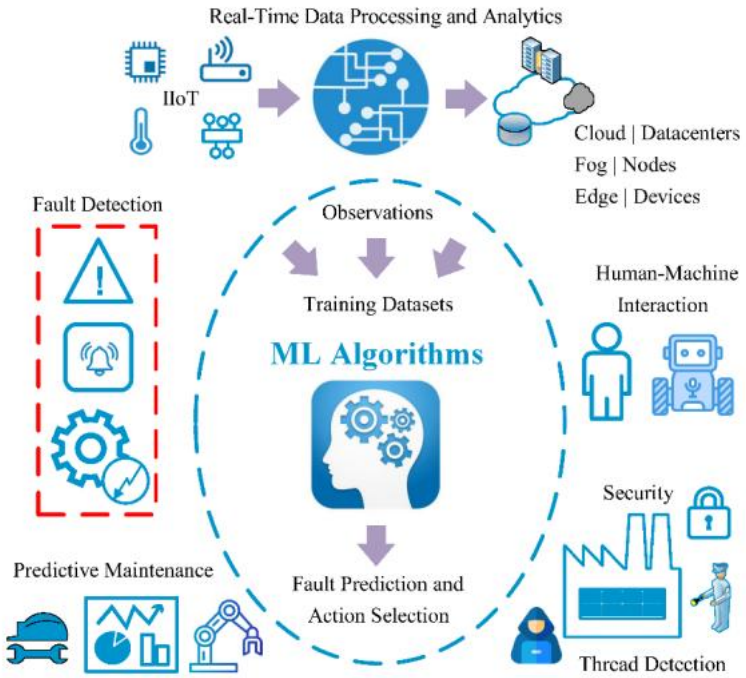

Figure 2: Dynamic Fault Diagnosis: Safeguarding Operational Integrity

Deployment of intrusion detection systems (IDS) is a crucial strategy for enhancing the cybersecurity of smart grids[73]. IDS are specialized security tools designed to monitor network traffic, detect suspicious or malicious activity, and alert security personnel to potential cyber threats in real-time[74]. The deployment of IDS in smart grid environments offers several key benefits and considerations: Continuous Monitoring: IDS continuously monitors network traffic and analyzes data packets for signs of anomalous behavior or known attack patterns[75]. By monitoring network traffic in real-time, IDS can detect and respond to potential cyber threats promptly, minimizing the impact of cyber-attacks on grid operations[76, 77]. Threat Detection: IDS is capable of detecting various types of cyber threats, including malware infections, denial-of-service (DoS) attacks, unauthorized access attempts, and data exfiltration[78]. By analyzing network traffic patterns and comparing them against predefined signatures or behavioral baselines, IDS can identify potential security incidents and raise alerts for further investigation[79]. Early Warning System: IDS serves as an early warning system for potential cyber threats, providing security personnel with timely alerts and notifications when suspicious

activity is detected[80]. This allows security teams to investigate and respond to security incidents promptly, mitigating the risk of cyber-attacks and minimizing the impact on grid operations. Customization and Tuning: IDS can be customized and tuned to meet the specific security requirements and operational characteristics of smart grid environments[81]. This includes defining custom rules, thresholds, and alerts based on the unique network architecture, communication protocols, and operational needs of the smart grid infrastructure[82]. Integration with Security Operations Center (SOC): IDS can be integrated with a centralized Security Operations Center (SOC) or Security Information and Event Management (SIEM) system to streamline security monitoring, analysis, and response activities[83, 84]. This enables security personnel to correlate and analyze security events from multiple sources, prioritize alerts, and coordinate incident response efforts effectively. Scalability and Flexibility: IDS solutions are scalable and flexible, allowing for deployment in distributed smart grid environments with varying levels of complexity and size. Whether deployed at the network perimeter, within the internal network, or at critical infrastructure points, IDS can adapt to the evolving cybersecurity needs of smart grid deployments[85]. Regulatory Compliance: Deployment of IDS helps utilities comply with regulatory requirements and cybersecurity standards, such as the NERC CIP standards. Many regulatory frameworks mandate the use of intrusion detection systems as part of a comprehensive cybersecurity program to protect critical infrastructure and ensure the reliability and security of the electric grid [86].

3. Fault Diagnosis Techniques for Resilience

Fault diagnosis plays a critical role in grid resilience by enabling utilities to swiftly detect, isolate, and address faults or abnormalities in the grid infrastructure[87]. Grid resilience refers to the ability of the power grid to withstand and recover from disruptions, such as equipment failures, natural disasters, cyber-attacks, or human errors, while maintaining the reliable delivery of electricity to consumers[88]. Here are several key reasons why fault diagnosis is crucial for grid resilience: Early Detection of Faults: Fault diagnosis techniques enable utilities to detect grid disturbances or equipment failures early, often before they escalate into larger-scale disruptions. Early detection allows utilities to initiate timely response measures, such as rerouting power flows, isolating affected areas, or implementing corrective actions, to minimize the impact on grid operations and prevent cascading failures[89, 90]. Minimization of Downtime: By identifying the root cause of grid faults or abnormalities quickly and accurately,

fault diagnosis helps utilities minimize downtime and restore service to affected areas promptly[91]. Rapid fault diagnosis enables utilities to deploy resources efficiently, prioritize restoration efforts, and expedite repairs or maintenance activities to restore grid functionality and reduce service interruptions. Optimization of Resources: Fault diagnosis facilitates the optimization of grid resources by providing utilities with insights into grid performance, equipment health, and operational conditions. By analyzing fault data and equipment performance metrics, utilities can prioritize maintenance activities, allocate resources effectively, and optimize grid operations to enhance system reliability and resilience[92]. Enhanced Situational Awareness: Fault diagnosis enhances utilities' situational awareness by providing real-time information and actionable intelligence about grid disturbances or abnormalities. Comprehensive fault diagnosis systems leverage advanced analytics and real-time monitoring to analyze grid data, identify anomalies, and generate actionable insights for operators and decision-makers, enabling proactive response strategies and informed decision-making during grid disturbances[93]. Resilience Planning: Fault diagnosis informs resilience planning efforts by helping utilities identify potential vulnerabilities, assess risk exposure, and develop contingency plans to mitigate the impact of grid disturbances[94]. By understanding the root causes of past failures and analyzing failure modes, utilities can strengthen grid resilience, improve system reliability, and enhance emergency response capabilities to withstand future disruption [95]. Improved Customer Satisfaction: By minimizing downtime and service interruptions, fault diagnosis contributes to improved customer satisfaction and trust in the reliability of the electric grid. Timely detection and resolution of grid faults ensure that customers receive uninterrupted electricity supply, thereby enhancing their overall experience and confidence in the utility's ability to deliver reliable service. Overall, fault diagnosis is essential for enhancing grid resilience by enabling utilities to detect, diagnose, and respond to grid disturbances promptly and effectively. By leveraging advanced fault diagnosis techniques and integrating fault diagnosis capabilities into grid operations, utilities can enhance system reliability, minimize downtime, and ensure the reliable delivery of electricity to consumers, even in the face of unforeseen events or disruptions[96].

Integrating fault diagnosis with cybersecurity measures is essential for enhancing the resilience of smart grids by enabling utilities to detect, diagnose, and respond to grid disturbances caused by both physical faults and cybersecurity threats[97]. Here's how the integration of fault

diagnosis with cybersecurity measures can be achieved: Comprehensive Monitoring: Integrate fault diagnosis systems with cybersecurity monitoring tools to provide comprehensive visibility into grid operations and cybersecurity events. By monitoring both the physical and cyber aspects of grid operations in real-time, utilities can detect and respond to grid disturbances caused by physical faults or cybersecurity incidents promptly. Anomaly Detection: Leverage data analytics techniques to identify anomalies or deviations from normal operating conditions that may indicate potential grid disturbances or cybersecurity threats[98]. By integrating fault diagnosis algorithms with cybersecurity anomaly detection systems, utilities can identify abnormal behavior across both physical and cyber domains, enabling proactive response strategies. Cyber-Physical Correlation: Establish correlations between cybersecurity events and physical grid operations to identify potential cause-and-effect relationships between cyber incidents and grid disturbances[99]. By correlating cybersecurity alerts with grid sensor data and control system events, utilities can identify cyber-physical attack vectors and assess the impact of cyber incidents on grid reliability and performance. Incident Response Coordination: Integrate incident response procedures and workflows between physical and cybersecurity teams to facilitate coordinated response efforts during grid disturbances[100]. By establishing communication channels and collaboration mechanisms between physical and cybersecurity personnel, utilities can streamline incident response coordination and mitigate the impact of grid disturbances more effectively. Cyber-Physical Resilience Planning: Develop cyber-physical resilience plans that consider the interdependencies between physical and cyber systems and address potential vulnerabilities across both domains. By incorporating fault diagnosis techniques and cybersecurity measures into resilience planning efforts, utilities can enhance grid resilience and ensure continuity of operations in the face of evolving threats and challenges. Overall, integrating fault diagnosis with cybersecurity measures is essential for enhancing the resilience of smart grids by enabling utilities to detect, diagnose, and respond to grid disturbances caused by both physical faults and cybersecurity threats. By adopting a holistic approach that considers the interconnected nature of physical and cyber systems, utilities can enhance grid reliability, minimize downtime, and ensure the reliable delivery of electricity to consumers, even in the face of complex and evolving threats.

4. Conclusion

In conclusion, the imperative to fortify smart grid cybersecurity and implement effective fault diagnosis strategies is paramount in ensuring the resilience of modern power grids. The evolving threat landscape necessitates a comprehensive approach that encompasses robust risk assessment, the deployment of advanced intrusion detection systems, and the adoption of secure communication protocols. Leveraging machine learning and artificial intelligence enhances the grid's ability to detect and respond to cyber threats swiftly. Additionally, integrating fault diagnosis techniques, such as data analytics and real-time monitoring, enables proactive identification and mitigation of grid disturbances. Collaboration among stakeholders, including utilities, government entities, academia, and industry players, is essential to fostering a cohesive cybersecurity ecosystem. By prioritizing these measures and fostering collaboration, smart grid operators can bolster resilience, safeguard critical infrastructure, and ensure uninterrupted energy delivery in the face of evolving threats.

Reference

[1] H. M. Khalid *et al.*, "WAMS operations in power grids: A track fusion-based mixture density estimation-driven grid resilient approach toward cyberattacks," *IEEE Systems Journal,* 2023.

[2] T. Nguyen, S. Wang, M. Alhazmi, M. Nazemi, A. Estebsari, and P. Dehghanian, "Electric power grid resilience to cyber adversaries: State of the art," *IEEE Access,* vol. 8, pp. 87592-87608, 2020.

[3] F. Mohammadi, "Emerging challenges in smart grid cybersecurity enhancement: A review," *Energies,* vol. 14, no. 5, p. 1380, 2021.

[4] Y. L. Jian and C. Luaus, "Enhancing Power Grid Security: A Comprehensive Study on Cybersecurity Measures and Fault Diagnosis Strategies Amid Dynamic System Variations," *Revista Espanola de Documentacion Cientifica,* vol. 17, no. 2, pp. 68-94, 2023.

[5] H. Khalid, F. Flitti, M. Mahmoud, M. Hamdan, S. Muyeen, and Z. Dong, "WAMS Operations in Modern Power Grids: A Median Regression Function-Based State Estimation Approach Towards Cyber Attacks," *El-Sevier–Sustainable Energy, Grid, and Networks,* vol. 34, p. 101009, 2023.

[6] A. Pasias, T. Kotsiopoulos, G. Lazaridis, A. Drosou, D. Tzovaras, and P. Sarigiannidis, "Cyber-Resilience Enhancement Framework in Smart Grids," in *Power Systems Cybersecurity: Methods, Concepts, and Best Practices*: Springer, 2023, pp. 363-386.

[7] A. D. Syrmakesis, C. Alcaraz, and N. D. Hatziargyriou, "Classifying resilience approaches for protecting smart grids against cyber threats," *International Journal of Information Security,* vol. 21, no. 5, pp. 1189-1210, 2022.

[8] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electric Power Systems Research,* vol. 215, p. 108975, 2023.

[9] M. Ghiasi, M. Dehghani, T. Niknam, and A. Kavousi-Fard, "Investigating the overall structure of cyber-attacks on smart-grid control systems to improve cyber resilience in power system," *Network,* vol. 1, no. 1, 2020.

[10] H. Khalid, S. Muyeen, and I. Kamwa, "Excitation Control for Multi-Area Power Systems: An Improved Decentralized Finite-Time Approach," *El-Sevier–Sustainable Energy, Grid, and Networks,* vol. 31, p. 100692, 2022.

[11] H. Shahinzadeh, A. Mahmoudi, J. Moradi, H. Nafisi, E. Kabalci, and M. Benbouzid, "Anomaly detection and resilience-oriented countermeasures against cyberattacks in smart grids," in *2021 7th International Conference on Signal Processing and Intelligent Systems (ICSPIS)*, 2021: IEEE, pp. 1-7.

[12] S. S. Ullah, A. J. Abianeh, F. Ferdowsi, K. Basulaiman, and M. Barati, "Measurable challenges in smart grid cybersecurity enhancement: A brief review," in *2021 IEEE Green Technologies Conference (GreenTech)*, 2021: IEEE, pp. 331-338.

[13] P. Wang and M. Govindarasu, "Multi-agent based attack-resilient system integrity protection for smart grid," *IEEE Transactions on Smart Grid,* vol. 11, no. 4, pp. 3447-3456, 2020.

[14] P. Zhao, C. Gu, Y. Ding, H. Liu, Y. Bian, and S. Li, "Cyber-resilience enhancement and protection for uneconomic power dispatch under cyber-attacks," *IEEE Transactions on Power Delivery,* vol. 36, no. 4, pp. 2253-2263, 2020.

[15] I. A. Iftimie and G. Huskaj, "Strengthening the cybersecurity of smart grids: The role of artificial intelligence in resiliency of substation intelligent electronic devices," in *Proceedings of the Nineteenth European Conference on Cyber Warfare and Security*, 2020, pp. 143-150.

[16] M. Mohammadpourfard, A. Khalili, I. Genc, and C. Konstantinou, "Cyber-resilient smart cities: Detection of malicious attacks in smart grids," *Sustainable Cities and Society,* vol. 75, p. 103116, 2021.

[17] H. M. Khalid, F. Flitti, S. Muyeen, M. S. Elmoursi, O. S. Tha'er, and X. Yu, "Parameter estimation of vehicle batteries in V2G systems: An exogenous function-based approach," *IEEE Transactions on Industrial Electronics,* vol. 69, no. 9, pp. 9535-9546, 2021.

[18] N. U. Ibne Hossain, M. Nagahi, R. Jaradat, C. Shah, R. Buchanan, and M. Hamilton, "Modeling and assessing cyber resilience of smart grid using Bayesian network-based approach: a system of systems problem," *Journal of Computational Design and Engineering,* vol. 7, no. 3, pp. 352-366, 2020.

[19] A. Rahiminejad *et al.*, "A resilience-based recovery scheme for smart grid restoration following cyberattacks to substations," *International Journal of Electrical Power & Energy Systems,* vol. 145, p. 108610, 2023.

[20] J. Chen *et al.*, "A multi-layer security scheme for mitigating smart grid vulnerability against faults and cyber-attacks," *Applied Sciences,* vol. 11, no. 21, p. 9972, 2021.

[21] M. M. Hosseini and M. Parvania, "Artificial intelligence for resilience enhancement of power distribution systems," *The Electricity Journal,* vol. 34, no. 1, p. 106880, 2021.

[22] F. Mohammadi, M. Saif, M. Ahmadi, and B. Shafai, "A review of cyber–resilient smart grid," in *2022 World Automation Congress (WAC)*, 2022: IEEE, pp. 28-35.

[23] U. Inayat, M. F. Zia, S. Mahmood, H. M. Khalid, and M. Benbouzid, "Learning-based methods for cyber attacks detection in IoT systems: A survey on methods, analysis, and prospects," *Electronics,* vol. 11, no. 9, p. 1502, 2022.

[24] T. Alsuwian, A. Shahid Butt, and A. A. Amin, "Smart grid cyber security enhancement: challenges and solutions—a review," *Sustainability,* vol. 14, no. 21, p. 14226, 2022.

[25] D. B. Unsal, T. S. Ustun, S. S. Hussain, and A. Onen, "Enhancing cybersecurity in smart grids: false data injection and its mitigation," *Energies,* vol. 14, no. 9, p. 2657, 2021.

[26] H. Badihi, "Smart Grid Resilience," in *Handbook of Smart Energy Systems*: Springer, 2023, pp. 1795-1819.

[27] M. Z. Gunduz and R. Das, "Cyber-security on the smart grid: Threats and potential solutions," *Computer networks,* vol. 169, p. 107094, 2020.

[28] Z. Rafique, H. M. Khalid, S. Muyeen, and I. Kamwa, "Bibliographic review on power system oscillations damping: An era of conventional grids and renewable energy integration," *International Journal of Electrical Power & Energy Systems,* vol. 136, p. 107556, 2022.

[29] U. Inayat, M. F. Zia, S. Mahmood, T. Berghout, and M. Benbouzid, "Cybersecurity enhancement of smart grid: Attacks, methods, and prospects," *Electronics,* vol. 11, no. 23, p. 3854, 2022.

[30] F. Alasali *et al.*, "Smart Grid Resilience for Grid-Connected PV and Protection Systems under Cyber Threats," *Smart Cities,* vol. 7, no. 1, pp. 51-77, 2023.

[31] E. Hossain, S. Roy, N. Mohammad, N. Nawar, and D. R. Dipta, "Metrics and enhancement strategies for grid resilience and reliability during natural disasters," *Applied Energy,* vol. 290, p. 116709, 2021.

[32] A. E. L. Rivas and T. Abrao, "Faults in smart grid systems: Monitoring, detection and classification," *Electric Power Systems Research,* vol. 189, p. 106602, 2020.

[33] S. Ashraf, M. H. Shawon, H. M. Khalid, and S. Muyeen, "Denial-of-service attack on IEC 61850-based substation automation system: A crucial cyber threat towards smart substation pathways," *Sensors,* vol. 21, no. 19, p. 6415, 2021.

[34] S. Dutta, S. K. Sahu, S. Dutta, and B. Dey, "Leveraging a micro synchrophasor for fault detection in a renewable-based smart grid—a machine-learned sustainable solution with cyber-attack resiliency," *e-Prime-advances in electrical engineering, electronics and energy,* vol. 2, p. 100090, 2022.

[35] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, A. Abusorrah, L. Che, and X. Liu, "Cross-layer distributed control strategy for cyber resilient microgrids," *IEEE Transactions on Smart Grid,* vol. 12, no. 5, pp. 3705-3717, 2021.

[36] A. Gumaei *et al.*, "A robust cyberattack detection approach using optimal features of SCADA power systems in smart grids," *Applied Soft Computing,* vol. 96, p. 106658, 2020.

[37] L. Xu, Q. Guo, Y. Sheng, S. Muyeen, and H. Sun, "On the resilience of modern power systems: A comprehensive review from the cyber-physical perspective," *Renewable and Sustainable Energy Reviews,* vol. 152, p. 111642, 2021.

[38] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, "CPIndex: Cyber-physical vulnerability assessment for power-grid infrastructures," *IEEE Transactions on Smart Grid,* vol. 6, no. 2, pp. 566-575, 2014.

[39] Y. B. Yusof, T. H. Ping, and F. B. M. Isa, "Strengthening Smart Grids Through Security Measures: A Focus on Real-Time Monitoring, Redundancy, and Cross-Sector Collaboration," *International Journal of Intelligent Automation and Computing,* vol. 6, no. 3, pp. 14-36, 2023.

[40] S. Tufail, I. Parvez, S. Batool, and A. Sarwat, "A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid," *Energies,* vol. 14, no. 18, p. 5894, 2021.

[41] Y. Song, C. Wan, X. Hu, H. Qin, and K. Lao, "Resilient power grid for smart city," *iEnergy,* vol. 1, no. 3, pp. 325-340, 2022.

[42] Z. Rafique, H. M. Khalid, and S. Muyeen, "Communication systems in distributed generation: A bibliographical review and frameworks," *IEEE Access,* vol. 8, pp. 207226-207239, 2020.

[43] F. Li, M. Valero, L. Zhao, and Y. Mahmoud, "Cybersecurity Strategy against Cyber Attacks towards Smart Grids with PVs," 2020.

[44] A. Qazzafi and G. Stiphen, "Navigating Cyber Threats: Enhancing Power Grid Resilience Through Advanced Cybersecurity and Dynamic Fault Diagnosis Techniques," *International Journal of Advanced Engineering Technologies and Innovations,* vol. 1, no. 03, pp. 1-31, 2023.

[45] M. Ghiasi, Z. Wang, T. Niknam, M. Dehghani, and H. R. Ansari, "Cyber-Physical Security in Smart Power Systems from a Resilience Perspective: Concepts and Possible Solutions," in *Power Systems Cybersecurity: Methods, Concepts, and Best Practices*: Springer, 2023, pp. 67-89.

[46] H. M. Khalid and J. C.-H. Peng, "Bidirectional charging in V2G systems: An in-cell variation analysis of vehicle batteries," *IEEE Systems Journal,* vol. 14, no. 3, pp. 3665-3675, 2020.

[47] Z. Liu and L. Wang, "Leveraging network topology optimization to strengthen power grid resilience against cyber-physical attacks," *IEEE Transactions on Smart Grid,* vol. 12, no. 2, pp. 1552-1564, 2020.

[48] P. Cicilio *et al.*, "Resilience in an evolving electrical grid," *Energies,* vol. 14, no. 3, p. 694, 2021.

[49] H. M. Khalid, S. Muyeen, and J. C.-H. Peng, "Cyber-attacks in a looped energy-water nexus: An inoculated sub-observer-based approach," *IEEE Systems Journal,* vol. 14, no. 2, pp. 2054-2065, 2019.

[50] D. Sarathkumar, M. Srinivasan, A. A. Stonier, R. Samikannu, N. R. Dasari, and R. A. Raj, "A technical review on self-healing control strategy for smart grid power systems," in *IOP conference series: materials science and engineering*, 2021, vol. 1055, no. 1: IOP Publishing, p. 012153.

[51] D. Hauer, D. Ratasich, L. Krammer, and A. Jantsch, "A methodology for resilient control and monitoring in smart grids," in *2020 IEEE International Conference on Industrial Technology (ICIT)*, 2020: IEEE, pp. 589-594.

[52] A. S. Musleh, H. M. Khalid, S. Muyeen, and A. Al-Durra, "A prediction algorithm to enhance grid resilience toward cyber attacks in WAMCS applications," *IEEE Systems Journal,* vol. 13, no. 1, pp. 710-719, 2017.

[53] B. W. Tuinema, J. L. Rueda Torres, A. I. Stefanov, F. M. Gonzalez-Longatt, and M. A. van der Meijden, "Cyber-physical system modeling for assessment and enhancement of power grid cyber security, resilience, and reliability," *Probabilistic Reliability Analysis of Power Systems: A Student's Introduction,* pp. 237-270, 2020.

[54] S. Tan, Y. Wu, P. Xie, J. M. Guerrero, J. C. Vasquez, and A. Abusorrah, "New challenges in the design of microgrid systems: Communication networks, cyberattacks, and resilience," *IEEE Electrification Magazine,* vol. 8, no. 4, pp. 98-106, 2020.

[55] N. D. Tuyen, N. S. Quan, V. B. Linh, V. Van Tuyen, and G. Fujita, "A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy," *IEEE Access,* vol. 10, pp. 35846-35875, 2022.

[56] H. T. Reda, A. Anwar, A. N. Mahmood, and Z. Tari, "A Taxonomy of Cyber Defence Strategies Against False Data Attacks in Smart Grids," *ACM Computing Surveys,* vol. 55, no. 14s, pp. 1-37, 2023.

[57] H. M. Khalid and J. C.-H. Peng, "Immunity toward data-injection attacks using multisensor track fusion-based model prediction," *IEEE Transactions on Smart Grid,* vol. 8, no. 2, pp. 697-707, 2015.

[58] J. Ruan *et al.*, "Deep learning for cybersecurity in smart grids: Review and perspectives," *Energy Conversion and Economics,* vol. 4, no. 4, pp. 233-251, 2023.

[59] P. U. Rao, B. Sodhi, and R. Sodhi, "Cyber Security Enhancement of Smart Grids Via Machine Learning-A Review," in *2020 21st National Power Systems Conference (NPSC)*, 2020: IEEE, pp. 1-6.

[60] A. Alamin, H. M. Khalid, and J. C.-H. Peng, "Power system state estimation based on Iterative Extended Kalman Filtering and bad data detection using the normalized residual test," in *2015 IEEE Power and Energy Conference at Illinois (PECI)*, 2015: IEEE, pp. 1-5.

[61] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "A cyber-attack resilient distributed control strategy in islanded microgrids," *IEEE Transactions on Smart Grid,* vol. 11, no. 5, pp. 3690-3701, 2020.

[62] S. Jadidi, H. Badihi, and Y. Zhang, "Active fault-tolerant and attack-resilient control for a renewable microgrid against power-loss faults and data integrity attacks," *IEEE Transactions on Cybernetics,* 2023.

[63] S. Mishra, K. Anderson, B. Miller, K. Boyer, and A. Warren, "Microgrid resilience: A holistic approach for assessing threats, identifying vulnerabilities, and designing corresponding mitigation strategies," *Applied Energy,* vol. 264, p. 114726, 2020.

[64] H. M. Khalid and J. C.-H. Peng, "A Bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks," *IEEE Transactions on Smart Grid,* vol. 7, no. 4, pp. 2026-2037, 2016.

[65] M. Z. Jahromi, A. A. Jahromi, S. Sanner, D. Kundur, and M. Kassouf, "Cybersecurity enhancement of transformer differential protection using machine learning," in *2020 IEEE Power & Energy Society General Meeting (PESGM)*, 2020: IEEE, pp. 1-5.

[66] X. Qin, K. Mai, N. Ortiz, K. Koneru, and A. A. Cardenas, "Cybersecurity and resilience for the power grid," *Resilient Control Architectures and Power Systems,* pp. 201-214, 2021.

[67] H. M. Khalid and J. C.-H. Peng, "Tracking electromechanical oscillations: An enhanced maximum-likelihood based approach," *IEEE Transactions on Power Systems,* vol. 31, no. 3, pp. 1799-1808, 2015.

[68] E. Shittu, A. Tibrewala, S. Kalla, and X. Wang, "Meta-analysis of the strategies for self-healing and resilience in power systems," *Advances in Applied Energy,* vol. 4, p. 100036, 2021.

[69] P. R. Grammatikis *et al.*, "Sdn-based resilient smart grid: The sdn-micro sense architecture," *Digital,* vol. 1, no. 4, pp. 173-187, 2021.

[70] M. Elsisi, C.-L. Su, and M. N. Ali, "Design of reliable IoT systems with deep learning to support resilient demand side management in smart grids against adversarial attacks," *IEEE Transactions on Industry Applications,* 2023.

[71] H. M. Khalid and J. C.-H. Peng, "Improved recursive electromechanical oscillations monitoring scheme: A novel distributed approach," *IEEE Transactions on Power Systems,* vol. 30, no. 2, pp. 680-688, 2014.

[72] Z. Chu, S. Lakshminarayana, B. Chaudhuri, and F. Teng, "Mitigating load-altering attacks against power grids using cyber-resilient economic dispatch," *IEEE Transactions on Smart Grid,* 2022.

[73] J. De La Cruz, E. Gómez-Luna, M. Ali, J. C. Vasquez, and J. M. Guerrero, "Fault location for distribution smart grids: Literature overview, challenges, solutions, and future trends," *Energies,* vol. 16, no. 5, p. 2280, 2023.

[74] R. Hemmati and H. Faraji, "Identification of cyber-attack/outage/fault in a zero-energy building with load and energy management strategies," *Journal of Energy Storage,* vol. 50, p. 104290, 2022.

[75] A. S. Musleh, M. Debouza, H. M. Khalid, and A. Al-Durra, "Detection of false data injection attacks in smart grids: A real-time principle component analysis," in *IECON 2019-45th Annual Conference of the IEEE Industrial Electronics Society*, 2019, vol. 1: IEEE, pp. 2958-2963.

[76] I. Srivastava, S. Bhat, and A. R. Singh, "Fault diagnosis, service restoration, and data loss mitigation through multi-agent system in a smart power distribution grid," *Energy Sources, Part A: Recovery, Utilization, and Environmental Effects,* pp. 1-26, 2020.

[77] K. Jalilpoor, M. T. Ameli, S. Azad, and Z. Sayadi, "Resilient energy management incorporating energy storage system and network reconfiguration: A framework of cyber-physical system," *IET Generation, Transmission & Distribution,* vol. 17, no. 8, pp. 1734-1749, 2023.

[78] A. S. Musleh, S. Muyeen, A. Al-Durra, and H. M. Khalid, "PMU based wide area voltage control of smart grid: A real-time implementation approach," in *2016 IEEE Innovative Smart Grid Technologies-Asia (ISGT-Asia)*, 2016: IEEE, pp. 365-370.

[79] B. Canaan, B. Colicchio, and D. Ould Abdeslam, "Microgrid cyber-security: Review and challenges toward resilience," *Applied Sciences,* vol. 10, no. 16, p. 5649, 2020.
[80] A. Khoukhi and M. H. Khalid, "Hybrid computing techniques for fault detection and isolation, a review," *Computers & Electrical Engineering,* vol. 43, pp. 17-32, 2015.
[81] S. Rath, T. Das, and S. Sengupta, "Improvise, Adapt, Overcome Dynamic Resiliency Against Unknown Attack Vectors in Microgrid Cybersecurity Games," *IEEE Transactions on Smart Grid,* 2024.
[82] M. K. Hasan, A. A. Habib, Z. Shukur, F. Ibrahim, S. Islam, and M. A. Razzaque, "Review on the cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations," *Journal of Network and Computer Applications,* vol. 209, p. 103540, 2023.
[83] M. Ghiasi, M. Dehghani, T. Niknam, A. Kavousi-Fard, P. Siano, and H. H. Alhelou, "Cyber-attack detection and cyber-security enhancement in smart DC-microgrid based on blockchain technology and Hilbert Huang transform," *Ieee Access,* vol. 9, pp. 29429-29440, 2021.
[84] M. S. Mahmoud and H. M. Khalid, "Data-driven fault detection filter design for time-delay systems," *International Journal of Automation and Control,* vol. 8, no. 1, pp. 1-16, 2014.
[85] O. A. Omitaomu and H. Niu, "Artificial intelligence techniques in smart grid: A survey," *Smart Cities,* vol. 4, no. 2, pp. 548-568, 2021.
[86] D. M. Menon, S. Sindhu, M. Manu, and S. Varma, "Cyber-Resilient Energy Infrastructure and IoT," in *Internet of Things, Artificial Intelligence and Blockchain Technology*: Springer, 2021, pp. 45-66.
[87] M. S. Mahmoud and H. M. Khalid, "Model prediction-based approach to fault-tolerant control with applications," *Ima Journal of mathematical control and Information,* vol. 31, no. 2, pp. 217-244, 2014.
[88] M. A. Ferrag, M. Babaghayou, and M. A. Yazici, "Cyber security for fog-based smart grid SCADA systems: Solutions and challenges," *Journal of Information Security and Applications,* vol. 52, p. 102500, 2020.
[89] T. Berghout, M. Benbouzid, and S. Muyeen, "Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects," *International Journal of Critical Infrastructure Protection,* p. 100547, 2022.
[90] M. S. Mahmoud and H. M. Khalid, "Expectation maximization approach to data-based fault diagnostics," *Information Sciences,* vol. 235, pp. 80-96, 2013.
[91] A. Althobaiti, A. Jindal, A. K. Marnerides, and U. Roedig, "Energy theft in smart grids: a survey on data-driven attack strategies and detection methods," *IEEE Access,* vol. 9, pp. 159291-159312, 2021.
[92] M. Mahmoud and H. Khalid, "Bibliographic review on distributed Kalman filtering," *IET Control Theory Appl,* vol. 7, no. 4, pp. 483-501, 2013.
[93] Z. Xu *et al.*, "A resilient defense strategy against false data injection attack in smart grid," in *2021 40th Chinese Control Conference (CCC)*, 2021: IEEE, pp. 4726-4731.
[94] A. Kemmeugne, A. A. Jahromi, and D. Kundur, "Resilience enhancement of pilot protection in power systems," *IEEE Transactions on Power Delivery,* vol. 37, no. 6, pp. 5255-5266, 2022.
[95] M. Rahim, H. M. Khalid, and M. Akram, "Sensor location optimization for fault diagnosis with a comparison to linear programming approaches," *The International Journal of Advanced Manufacturing Technology,* vol. 65, pp. 1055-1065, 2013.
[96] S. A. A. Abir, A. Anwar, J. Choi, and A. Kayes, "Iot-enabled smart energy grid: Applications and challenges," *IEEE Access,* vol. 9, pp. 50961-50981, 2021.
[97] V. K. Singh and M. Govindarasu, "A novel architecture for attack-resilient wide-area protection and control system in smart grid," in *2020 Resilience Week (RWS)*, 2020: IEEE, pp. 41-47.

[98] E. L. Ratnam, K. G. Baldwin, P. Mancarella, M. Howden, and L. Seebeck, "Electricity system resilience in a world of increased climate change and cybersecurity risk," *The Electricity Journal,* vol. 33, no. 9, p. 106833, 2020.

[99] M. Rahim, H. M. Khalid, and A. Khoukhi, "Nonlinear constrained optimal control problem: a PSO–GA-based discrete augmented Lagrangian approach," *The International Journal of Advanced Manufacturing Technology,* vol. 62, pp. 183-203, 2012.

[100] X. Liu, B. Chen, C. Chen, and D. Jin, "Electric power grid resilience with interdependencies between power and communication networks–a review," *IET Smart Grid,* vol. 3, no. 2, pp. 182-193, 2020.