frontiers | Frontiers in Energy Research

TYPE Mini Review
PUBLISHED 12 September 2023
DOI 10.3389/fenrg.2023.1274451

Check for updates

OPEN ACCESS

EDITED BY
Kumaran Kadirgama,
Universiti Malaysia Pahang, Malaysia

REVIEWED BY
Rui Wang,
Northeastern University, China

*CORRESPONDENCE
Fouzi Harrou,
Fouzi.harrou@kaust.edu.sa

RECEIVED 08 August 2023
ACCEPTED 31 August 2023
PUBLISHED 12 September 2023

CITATION
Harrou F, Taghezouit B, Bouyeddou B and Sun Y (2023), Cybersecurity of photovoltaic systems: challenges, threats, and mitigation strategies: a short survey.
Front. Energy Res. 11:1274451.
doi: 10.3389/fenrg.2023.1274451

COPYRIGHT
© 2023 Harrou, Taghezouit, Bouyeddou and Sun. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

Cybersecurity of photovoltaic systems: challenges, threats, and mitigation strategies: a short survey

Fouzi Harrou[1]*, Bilal Taghezouit[2], Benamar Bouyeddou[3] and Ying Sun[1]

[1]King Abdullah University of Science and Technology (KAUST) Computer, Electrical and Mathematical Sciences and Engineering (CEMSE) Division, Thuwal, Saudi Arabia, [2]Centre de Développement des Energies Renouvelables, Route de l'Observatoire, Algiers, Algeria, [3]LESM Lab, Faculty of Technology, University of Saida-Dr Moulay Tahar, Saida, Algeria

Photovoltaic (PV) systems, as critical components of the power grid, have become increasingly reliant on standard Information Technology (IT) computing and network infrastructure for their operation and maintenance. However, this dependency exposes PV systems to heightened vulnerabilities and the risk of cyber-attacks. In recent times, the number of reported cyber-attacks targeting PV systems has increased significantly. This paper provides an overview of the cybersecurity challenges faced by PV systems, emphasizing their susceptibility to anomalies and cyber threats. It highlights the urgency of implementing robust cybersecurity measures to protect the integrity and reliability of PV installations. By understanding and addressing these challenges, stakeholders can ensure the resilience and secure integration of PV systems within the power grid infrastructure.

KEYWORDS

photovoltaic systems, cybersecurity, vulnerabilities, attacks, AI methods

1 Introduction

Renewable energy systems, particularly solar photovoltaic (PV) installations, have emerged as a transformative force in the global energy landscape, providing sustainable alternatives to traditional fossil fuel-based generation (Jäger-Waldau, 2022). The solar PV market has experienced significant growth, reaching an installed capacity of 1185 GW in 2022, with 243 GW added in that year alone (IEA-PVPS, 2023). This growth is attributed to technological advancements, increased competitiveness, rising electricity demand, and favorable investment returns (Gantner Instruments, 2015). PV systems leverage cutting-edge technologies, including advanced controls, digital sensors, and sophisticated network architectures, to optimize energy efficiency, enable real-time monitoring, and seamlessly integrate with smart grids, creating a more dynamic and responsive energy ecosystem. These developments highlight the pivotal role of solar PV in meeting global energy needs while promoting sustainability.

As the adoption of PV systems continues to rise, their vulnerability to cybersecurity threats also increases. Over the past decade, cyberattacks have become pervasive across industries, including energy sector (Walker et al., 2021). Undetected cyberattacks on PV installations can lead to severe consequences, such as operational disruptions, financial losses, and even compromising broader energy infrastructure reliability. An illustrative example is the 2015 cyberattack on Ukraine's power grid, where hackers targeted control systems, triggering widespread outages affecting approximately 225,000 customers (Zetter, 2016). Similarly, a 2019 attack on a US utility impacted PV and wind installations due to an unpatched firewall breach, temporarily disrupting Supervisory Control and Data Acquisition (SCADA) systems and 500 MW of generation (Walker et al., 2021). These incidents emphasize the urgent need for robust cybersecurity measures in PV systems to avert future threats, underlining power grid vulnerability and potential repercussions of cyberattacks on vital systems.

Recent years have seen an increased emphasis on bolstering the cybersecurity of smart grids, leading to research efforts to identify and counter cyberattacks on grid components (Tuyen et al., 2022). However, there is a notable lack of studies specifically addressing cyberattack in PV plants (Walker et al., 2021; Ye et al., 2022). While PV systems are integral to the broader smart grid context as distributed energy resources, their distinct attributes necessitate focused research on effective cyberattack detection and mitigation strategies. PV systems are complex due to their intermittency and reliance on environmental factors, resulting in unpredictable power generation patterns. This complexity challenges the identification of normal versus compromised behavior, demanding tailored cybersecurity algorithms. The intermittent nature of PV generation creates a random signal environment that can aid attackers in evading detection (Ye et al., 2022). The core of PV systems, the solar inverter, acts as a crucial interface between panels and the grid. While these inverters offer advanced functions, they also present vulnerabilities that, if exploited, could severely impact both PV system operation and the overall electrical grid's stability and security (Kang et al., 2015).

The increasing complexity of interconnected PV systems introduces cybersecurity challenges. Various components like advanced meters, inverters, sensors, and control systems pose vulnerability risks. Ensuring system integrity and resilience requires efficient cybersecurity measures. Despite limited studies, recent research has started focusing on PV system cybersecurity to enhance smart grid protection. (Li et al., 2021). introduce a diagnostic solution based on deep sequence learning to address data integrity attacks targeting PV systems within smart grids. This approach utilizes time-series electric waveform data obtained from current and voltage sensors. (Miranda and Goldsmith, 2017). present a risk assessment approach to evaluate the cybersecurity posture of a grid-connected commercial PV plant, examining vulnerabilities and attack vectors specific to its Industrial Control System (ICS) architecture. (Liu et al., 2017). developed a risk assessment method considering the impact of cyber-attacks on microgrid control systems, particularly focusing on PV and energy storage system (ESS) control systems. (Ye et al., 2022). analyze the prospects and challenges of cyber-physical security in PV systems, exploring different cyber-attacks and outlining techniques that involve model-driven and data-driven approaches to identify and counter threats. (Choi et al., 2021). propose a blockchain-based Man-In-The-Middle (MITM) attack detection method for PV systems, enhancing data integrity and security during communication. (Larkin et al., 2020). explore the cybersecurity protections of data diodes for typical PV systems, assessing economic considerations for their deployment. (Shen et al., 2019). present a robust control architecture for mitigating sensor and actuator attacks on PV converter systems, enhancing resilience against cyber-physical attacks. (Zhao et al., 2022). propose a federated learning strategy to detect false data injection attacks in solar farms, offering an efficient decentralized approach for PV system security. While limited, these studies represent significant strides toward bolstering the cybersecurity of PV systems and smart grids. Further research in this emerging area is important to ensure the secure and reliable integration of PV systems into the energy landscape (Kang et al., 2015; Jones et al., 2021).

This short review paper sheds light on the evolving cybersecurity landscape for PV systems, emphasizing their growing vulnerability to cyber threats as they integrate into modern energy grids. Existing research has focused more on smart grids, leaving PV systems with limited attention. The paper briefly reviews recent solutions and discusses ongoing challenges, urging further research to develop tailored cybersecurity algorithms for PV systems' intermittent behavior.

2 Threat landscape and cyberattack detection for photovoltaic systems

2.1 Threat landscape for PV systems

Solar PV technology presents distinct challenges compared to wind-based systems due to its versatility and wide range of applications. PV systems can be utilized in various settings, including large-scale solar plants, industrial and commercial medium-sized plants, and smaller residential installations. This diverse deployment of solar PV introduces complexity to the overall structure and may increase potential vulnerabilities (Johnson, 2017). The cyber-physical perspective of PV-based power systems identifies several potential attack points, as illustrated in Figure 1.

The threat landscape for PV systems is continuously evolving, with cyber attackers becoming more sophisticated and targeting various components and communication channels of these critical energy installations (Tertytchny et al., 2020). Denial of Service (DoS), Distributed DoS (DDoS), Data Integrity Attacks (DIAs) and MITM attacks, are some of the major threats facing PV systems. However, DIAs encompass various types of attacks, including False Data Injection Attacks (FDIAs), Covert Attack (CA), and Replay Attack (RA). In addition to cyberattacks, physical attacks against PV systems can be used to steal data, damage equipment or interrupt power supply.

Understanding the nature of threats is key to effective cybersecurity for PV installations. Robust measures like intrusion detection, secure protocols, and continuous monitoring are essential to safeguard against evolving cyber risks.

DoS and DDoS attacks are prevalent threats to PV systems, overwhelming them with excessive malicious requests (Zhong et al., 2017; Huseinović et al., 2020). In DoS, single-source attacks target various PV components, such as servers, communication channels, sensors, and monitoring interfaces, inundating them with overwhelming data packets or requests. On the other hand, DDoS uses multiple devices for simultaneous attacks, making the source harder to trace (Ye et al., 2022). Both attacks disrupt communication channels, inverters, data transmission, and control, impacting system performance and power output fluctuations. In

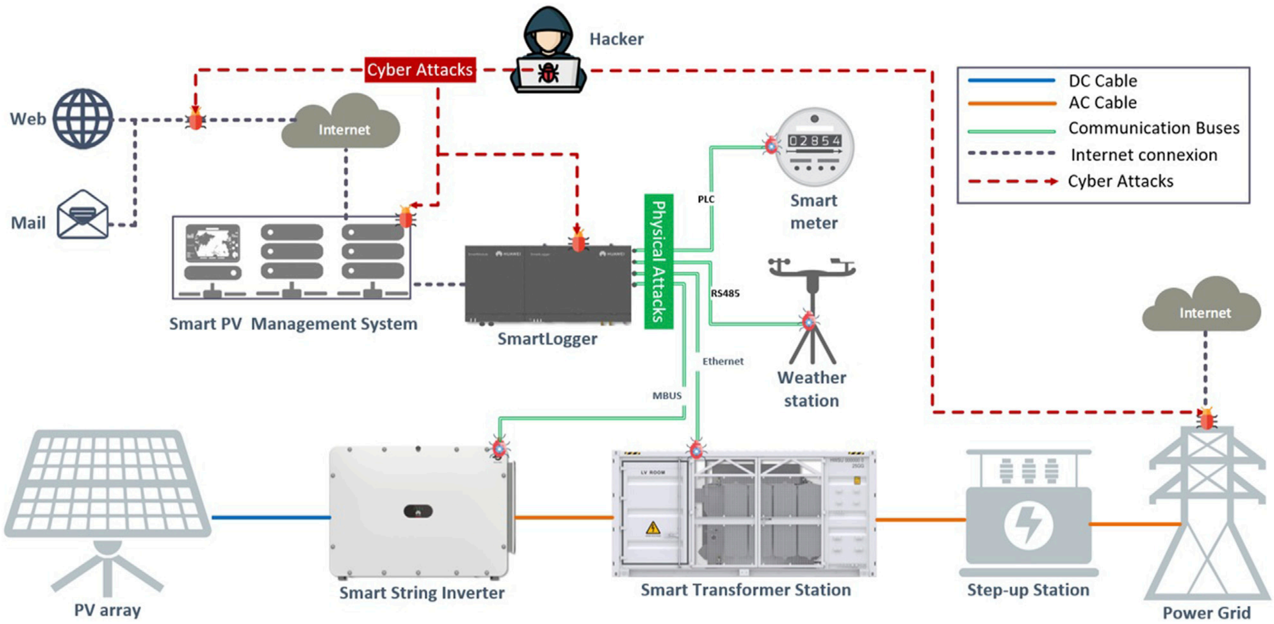

FIGURE 1
Possible vulnerabilities related to cyber and physical attacks in grid-connected PV plants.

contrast, Replay attacks involve intercepting and recording legitimate data exchanges between PV components and later replaying them to deceive the system into accepting them as current and authentic data (Ahmed et al., 2022). Attackers can capture control commands and manipulate system operations (Zhang et al., 2022). This can lead to unintended actions, disruptions, and compromised grid stability. On the other hand, DIAs in PV systems involve data integrity tampering, leading to inaccurate control decisions and system operation (Li et al., 2021; Zhang et al., 2022). Attackers manipulate sensor readings, alter control commands, inject false data, and falsify energy production data (Riggs et al., 2021), impacting grid stability and efficiency. Additionally, Stealthy cyber-attacks are designed to evade detection and operate covertly over extended periods, unlike typical attacks that cause immediate disruptions (Khazaei and Asrari, 2022). These attacks utilize techniques like Advanced Persistent Threats (APTs), Zero-Day Exploits, Data Exfiltration, Backdoor Access, and Fileless Malware. APTs employ sophisticated methods for long-term access, while Zero-Day Exploits target unknown vulnerabilities without triggering alarms. Data Exfiltration silently steals sensitive data, Backdoor Access maintains ongoing control, and Fileless Malware poses challenges for traditional antivirus solutions. The discovery and mitigation of stealthy attacks in PV systems require advanced threat detection and prevention mechanisms to counter the significant risks they pose. In addition to cyber-attacks, faults in PV systems, such as open-circuits, short-circuits, and inverter disconnections, can also have serious consequences and cast a shadow on system performance (Taghezouit et al., 2020; Harrou et al., 2021). If these faults go undetected for extended periods, they may result in reduced power generation efficiency, equipment damage, and potential disruptions in power supply. Therefore, implementing effective fault detection and rapid response mechanisms is essential to maintain the reliability and resilience of PV systems and ensure their optimal operation (Taghezouit et al., 2021; Harrou et al., 2022).

2.2 Cyberattack detection for photovoltaic systems

Advanced intrusion detection and prevention mechanisms such as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are crucial to detect cyberattacks on PV systems (Shen et al., 2019). These systems continuously monitor network traffic and system behaviors, analyzing patterns and anomalies to identify potential attacks in real time (Peng et al., 2023). Timely detection allows PV system operators to respond promptly and limit damage, safeguarding critical operations. However, the absence of robust security measures like encryption and firewalls makes PV systems vulnerable to unauthorized access and data breaches, while poorly secured communication networks offer opportunities for attackers to manipulate sensitive data.

Over the past decade, diverse cybersecurity strategies have emerged to safeguard grid-tied PV systems from evolving cyber threats. These approaches fall into two main categories: model-based and data-based methods. Model-based strategies utilize analytical models, which are usually developed based on some fundamental understanding of the system, to detect abnormal behavior, and threats. Numerous model-based methods for detecting cyber-attacks in PV systems have been developed. (Bai et al., 2020). conducted a quantitative assessment of threats using Semantic Web technology to analyze possible attacks on new energy plants, including PV power plants, from various perspectives. (Patel et al., 2021). proposed a dynamic loop wide-area damping strategy to enhance power system resilience against detectable and stealth cyber-attacks. (Huang et al., 2020). presented a defense mechanism based on dynamic watermarking to detect cyber anomalies in renewable-rich microgrids, proving its effectiveness through validation in a real microgrid. (Zhao et al., 2022). introduced a cross-layer control strategy to bolster microgrid resilience against FDI and DoS attacks. They validated the stability and efficacy of

TABLE 1 An overview of various defense techniques used against DIAs and DoS in smart grid and PV systems.

Vulnerability and attacks on	References	Techniques	Against DIAs	Against DoS
Inverters and Controllers	Ibrahim et al. (2022)	Dynamic watermarking	✓	
	Patel et al. (2021)	Sliding mode observer	✓	✓
	Beg et al. (2021)	Signal temporal logic	✓	✓
	Qiu et al. (2023)	synchrosqueezed wavelet transforms and recurrent layer aggregation-based CNN	✓	
Wide Area Monitoring, Protection and Control (WAMPAC) applications	Adeli et al. (2022)	Variation mode decomposition	✓	✓
	Beg et al. (2019)	Common path mining	✓	✓
Communication System	Huang et al. (2020)	Distributed watermarking	✓	
	Zhou et al. (2021)	Resilient economic control	✓	
	Singh and Govindarasu (2021)	Kullback-Leibler divergence	✓	✓
	Lu et al. (2021)	Isolation forest	✓	
	Hasnat and Rahnamay-Naeini (2021)	Multiclass support vector machine	✓	✓
Metering Infrastructure	Forti et al. (2018)	Linear regression	✓	
	Habibi et al. (2022)	K-Nearest Neighbour	✓	
	Zegeye et al. (2019)	Hidden Markov model	✓	
	Choi and Song (2006), Abdallah and Shen (2016)	Public key cartography	✓	
	Ma (2005), Kordestani and Saif (2021)	Puzzle based mechanisms		✓
	Tan et al. (2020)	Butterworth low pass filter	✓	✓
Internet of things (IoT) devices	Wei et al. (2019)	Evolutionary deep belief network	✓	
PCC voltages of Grid-tied PV System	Peng et al. (2023)	fast Fourier transform and multi-layer long short-term memory	✓	
Energy Management System (EMS)	Ahmed et al. (2019)	Isolation forest	✓	
	Li et al. (2017)	deep belief network	✓	

this strategy through simulation experiments. (Mustafa et al., 2020). introduced a resilient control framework for AC microgrids, countering data manipulation attacks using a Kullback-Leibler divergence-based approach. (Zhang et al., 2022). considered a physics-data-driven strategy via power electronics-enabled harmonic state space models to detect various cyber-attacks in PV farms, providing accurate detection and attack source localization within the farm. These dynamics-centered approaches employ models to detect and counter cyber-attacks on PV systems. However, developing accurate models for large PV systems is challenging due to their complexity and dynamics.

In contrast, data-based cybersecurity approaches in PV systems rely on historical data to create predictive models and identify anomalies. By employing machine learning algorithms and statistical techniques, they analyze system performance, communication patterns, and operational behavior using past data. Leveraging big data, these data-driven approaches demonstrate exceptional performance (Wang W. et al., 2022; Dairi et al., 2023), making them appealing for large-scale PV installations where accurate analytical models might be challenging to construct. Several data-based cybersecurity methods for PV systems have been proposed in recent research. An approach involves employing the Parametric Time-Frequency Logic (PTFL) framework to identify cyber-physical anomalies within microgrids. These anomalies encompass FDI attacks, DoS attacks, and faults occurring in power electronics devices, all within a controller/hardware-in-the-loop environment (Beg et al., 2021). Another method involves the use of synchro phasor measurements and network packet properties to develop a Cyber-Physical Anomaly Detection System (CPADS) for wide-area protection in control center-based centralized remedial action schemes (Singh and Govindarasu, 2021). Additionally, an evolutionary Deep Belief Network (DBN) approach, called PEO-DBN, has been proposed to detect cyber-attacks in industrial automation and control systems (Lu et al., 2021). Moreover, research has explored the monitoring of smart grids and detecting cyber and physical stresses using k-nearest neighbor classification based on instantaneous correlations of state components (Hasnat and Rahnamay-Naeini, 2021). To tackle FDI attacks in smart grids, a DBN-based scheme has been introduced, which outperforms existing classifiers (Wei et al., 2019; Jones et al., 2021) implemented another approach utilizing an Adaptive Resonance Theory (ART) artificial neural network. This technique focuses on safeguarding internet-connected PV inverters by using unsupervised online anomaly detection. Furthermore, comprehensive studies have been conducted on cyber-attack detection and diagnosis for PV farms using time-frequency domain features to distinguish between normal conditions, open-circuit faults, short-circuit faults, and cyber-attacks (Guo et al., 2022). Finally, a transfer learning approach has been proposed for detecting cyber-attacks in PV systems with less training data, resulting in better accuracy and faster convergence (Li et al., 2022).

In addition to the above, there are further studies on cybersecurity methods for PV systems. One research presents a Signal Temporal Logic (STL) detection method for False Data Injection Attacks (FDIAs) and DoS attacks in distributed cooperative control strategies in DC microgrids (Beg et al., 2019). Another paper proposes a data-driven detection framework based on support vector machine (SVM) to identify FDIAs against voltage regulation in PV-integrated power distribution systems (Ahmadzadeh et al., 2022). Moreover, a study addresses the challenge of detecting cyber-attacks originating from distributed edge devices, such as PV systems, using machine learning techniques (Sourav et al., 2022). Furthermore, researchers have explored data-driven methods on micro-Phasor Measurement Unit (μPMU) data to detect cyber-attacks in power electronics-enabled smart grids, achieving high accuracy using convolutional neural network (CNN) models (Li et al., 2020). Lastly, an anomaly detection strategy based on the physical behavior of the PV system has been proposed, employing a neural network architecture called autoencoder to detect possible cyber-attacks or faults (Gaggero et al., 2020). These research efforts contribute to enhancing the cybersecurity of PV systems, ensuring their stability and resilience against potential cyber threats. (Ahmed et al., 2019). propose an unsupervised machine learning-based scheme using isolation forest to detect covert data integrity assaults in smart grid communications networks, improving attack detection accuracy on standard IEEE power systems. This approach addresses cybersecurity concerns in modern smart grids. (Zegeye et al., 2019). present a multi-layer Hidden Markov Model-based Intrusion Detection System, leveraging machine learning algorithms to improve network defense against intruders, particularly in the context of next-generation (5G) networks. The multi-layer approach resolves the curse of dimensionality and captures multi-phase attacks over longer spans of time, offering actionable information to identify and respond to intrusions. Table 1 presents a compilation of recent studies that employ both model-based and data-based cybersecurity approaches to combat DIAs and DoS in smart grid and PV systems.

3 Discussion

The widespread adoption of PV systems in the energy sector is driven by technological advancements, cost-effectiveness, and environmental concerns. However, this expansion exposes these systems to potential cyber threats that can disrupt operations and impact the energy infrastructure. As PV systems integrate into the grid and rely on digital technologies, vulnerabilities arise from outdated components, weak security measures, and unsecured access points. Employing a multi-layered approach with Intrusion Detection and Prevention Systems (IDS/IPS) is essential. These systems monitor network activity in real-time, enabling swift response to cyber threats and safeguarding system reliability and resilience.

To strengthen PV system cybersecurity, vital strategies must be adopted. This includes robust security measures like encryption, firewalls, and secure communication protocols to thwart unauthorized access and data breaches. Regular software updates and patch management are vital to address vulnerabilities and bolster system resilience. Moreover, important are user training and awareness programs to empower operators and personnel in identifying and countering potential cyber threats.

Future research efforts should focus on addressing the unique challenges posed by PV systems' intermittent behavior and evolving cyber threats. Integrating advanced technologies, including Artificial Intelligence (AI) and Internet of things (IoT), will facilitate real-time detection and prevention of sophisticated cyberattacks. Collaboration among industry stakeholders, policymakers, and cybersecurity experts will be instrumental in developing standardized guidelines and protocols specific to PV system cybersecurity.

Another aspect to be considered is the integration of current sharing and voltage regulation in PV systems that optimizes power performance (Wang et al., 2020; Wang et al., 2022). However, rising cybersecurity risks pose threats to this harmony. Cyberattacks targeting control mechanisms and communication networks can disrupt these functions, impacting power distribution and system stability. Addressing this challenge requires a holistic approach that aligns current sharing, voltage regulation, and cybersecurity measures. Ensuring the reliability of control algorithms and communication protocols is vital to maintaining accurate current sharing and voltage regulation. Enhancing cyber resilience through regular updates and intrusion detection safeguards these processes. Ultimately, the interconnectedness of these functions underscores the need for a comprehensive strategy that prioritizes both technical efficiency and cybersecurity resilience.

Author contributions

FH: Conceptualization, Investigation, Supervision, Writing–original draft, Writing–review and editing. BT: Conceptualization, Investigation, Visualization, Writing–original draft, Writing–review and editing. BB: Conceptualization, Investigation, Writing–review and editing. YS: Conceptualization, Investigation, Resources, Supervision, Writing–review and editing.

Funding

The author(s) declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Abdallah, A., and Shen, X. S. "Efficient prevention technique for false data injection attack in smart grid," in Proceedings of the 2016 IEEE International Conference on Communications, ICC, Kuala Lumpur, Malaysia, May 2016. doi:10.1109/ICC.2016.7510610

Adeli, M., Hajatipour, M., Yazdanpanah, M. J., Hashemi-Dezaki, H., and Shafieirad, M. (2022). Optimized cyber-attack detection method of power systems using sliding mode observer. *Electr. Power Syst. Res.* 205, 107745. doi:10.1016/j.epsr.2021.107745

Ahmadzadeh, M., Abazari, A., and Ghafouri, M. "Detection of FDI attacks on voltage regulation of PV-integrated distribution grids using machine learning methods," in Proceedings of the 2022 IEEE Electrical Power and Energy Conference, Victoria, BC, Canada, December 2022. doi:10.1109/EPEC56903.2022.10000189

Ahmed, C. M., Palleti, V. R., and Mishra, V. K. (2022). A practical physical watermarking approach to detect replay attacks in a CPS. *J. Process Control* 116, 136–146. doi:10.1016/j.jprocont.2022.06.002

Ahmed, S., Lee, Y., Hyun, S. H., and Koo, I. (2019). Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest. *IEEE Trans. Inf. Forensics Secur* 14, 2765–2777. doi:10.1109/TIFS.2019.2902822

Beg, O. A., Nguyen, L. V., Johnson, T. T., and Davoudi, A. (2019). Signal temporal logic-based attack detection in DC microgrids. *IEEE Trans. Smart Grid* 10, 3585–3595. doi:10.1109/TSG.2018.2832544

Bai, X., Liu, L., Wei, D., and Cao, J. "Research on security threat and evaluation model of new energy plant and station," in Proceedings - 2020 International Conference on Computer Communication and Network Security, Xi'an, China, August 2020. doi:10.1109/CCNS50731.2020.00025

Beg, O. A., Nguyen, L. V., Johnson, T. T., and Davoudi, A. (2021). Cyber-physical anomaly detection in microgrids using time-frequency logic formalism. *IEEE Access* 9, 20012–20021. doi:10.1109/ACCESS.2021.3055229

Choi, J., Ahn, B., Bere, G., Ahmad, S., Mantooth, H. A., and Kim, T. "Blockchain-based man-in-the-middle (MITM) attack detection for photovoltaic systems," in Proceedings of the 2021 IEEE Design Methodologies Conference, Bath, United Kingdom, July 2021. doi:10.1109/DMC51747.2021.9529949

Choi, K. J., and Song, J. I. "Investigation of feasible cryptographic algorithms for wireless sensor network," in Proceedings of the 8th International Conference Advanced Communication Technology, Phoenix Park, February 2006. doi:10.1109/icact.2006.206229

Dairi, A., Harrou, F., Bouyeddou, B., Senouci, S. M., and Sun, Y. (2023). "Semi-supervised deep learning-driven anomaly detection schemes for cyber-attack detection in smart grids," in *Power systems* (Berlin, Germany: Springer). doi:10.1007/978-3-031-20360-2_11

Forti, N., Battistelli, G., Chisci, L., Li, S., Wang, B., and Sinopoli, B. (2018). Distributed joint attack detection and secure state estimation. *IEEE Trans. Signal Inf. Process. over Netw.* 4, 96–110. doi:10.1109/TSIPN.2017.2760804

Gaggero, G. B., Rossi, M., Girdinio, P., and Marchese, M. (2020). Detecting system fault/cyberattack within a photovoltaic system connected to the grid: A neural network-based solution. *J. Sens. Actuator Netw.* 9, 20. doi:10.3390/jsan9020020

Gantner Instruments, (2015). *Effective plant monitoring promotes efficient PV*. San Diego, CA, USA: Gantner Instruments.

Guo, L., Zhang, J., Ye, J., Coshatt, S. J., and Song, W. (2022). Data-driven cyber-attack detection for PV farms via time-frequency domain features. *IEEE Trans. Smart Grid* 13, 1582–1597. doi:10.1109/TSG.2021.3136559

Habibi, M. R., Baghaee, H. R., Blaabjerg, F., and Dragicevic, T. (2022). Secure MPC/ANN-Based false data injection cyber-attack detection and mitigation in DC microgrids. *IEEE Syst. J.* 16, 1487–1498. doi:10.1109/JSYST.2021.3086145

Harrou, F., Saidi, A., Sun, Y., and Khadraoui, S. (2021). Monitoring of photovoltaic systems using improved kernel-based learning schemes. *IEEE J. Photovoltaics* 11, 806–818. doi:10.1109/JPHOTOV.2021.3057169

Harrou, F., Taghezouit, B., Khadraoui, S., Dairi, A., Sun, Y., and Hadj Arab, A. (2022). Ensemble learning techniques-based monitoring charts for fault detection in photovoltaic systems. *Energies* 15, 6716–6728. doi:10.3390/en15186716

Hasnat, M. A., and Rahnamay-Naeini, M. (2021). Detecting and locating cyber and physical stresses in smart grids using the k-nearest neighbour analysis of instantaneous correlation of states. *IET Smart Grid* 4, 307–320. doi:10.1049/stg2.12030

Huang, T., Wang, B., Ramos-Ruiz, J., Enjeti, P., Kumar, P. R., and Xie, L. "Detection of cyber attacks in renewable-rich microgrids using dynamic watermarking," in Proceedings of the IEEE Power and Energy Society General Meeting, Montreal, QC, Canada, August 2020. doi:10.1109/PESGM41954.2020.9282071

Huseinović, A., Mrdović, S., Bicakci, K., and Uludag, S. (2020). A survey of denial-of-service attacks and solutions in the smart grid. *IEEE Access* 8, 177447–177470. doi:10.1109/ACCESS.2020.3026923

Ibrahim, H., Kim, J., Enjeti, P., Kumar, P. R., and Xie, L. "Detection of cyber attacks in grid-tied PV systems using dynamic watermarking," in Proceedings of the IEEE Green Technol. Conf., Houston, TX, USA, March 2022, 57–61. doi:10.1109/GreenTech52845.2022.9772036

IEA-PVPS (2023). Snapshot of global PV markets 2023. Available at: http://www.iea-pvps.org/fileadmin/dam/public/report/technical/PVPS_report_-_A_Snapshot_of_Global_PV_-_1992-2014.pdf.

Jäger-Waldau, A. (2022). Snapshot of photovoltaics - february 2022. *EPJ Photovoltaics* 13, 9. doi:10.1051/epjpv/2022010

Johnson, J. (2017). Roadmap for photovoltaic cyber security. *Sandia Natl. Lab.* Available at: http://sunspec.org/wp-content/uploads/2017/08/RoadmapforPhotovoltaicCyberSecurity-DraftforReview.pdf.

Jones, C. B., Chavez, A., Hossain-Mckenzie, S., Jacobs, N., Summers, A., and Wright, B. "Unsupervised online anomaly detection to identify cyber-attacks on internet connected photovoltaic system inverters," in Proceedings of the 2021 IEEE Power Energy Conf. Illinois, PECI, Urbana, IL, USA, April 2021, 1–7. doi:10.1109/PECI51586.2021.9435234

Kang, B. J., Maynard, P., McLaughlin, K., Sezer, S., Andrén, F., Seitl, C., et al. "Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations," in Proceedings of the IEEE International Conference on Emerging Technologies and Factory Automation, Luxembourg, Luxembourg, September 2015. doi:10.1109/ETFA.2015.7301457

Khazaei, J., and Asrari, A. (2022). Second-order cone programming relaxation of stealthy cyberattacks resulting in overvoltages in cyber-physical power systems. *IEEE Syst. J.* 16, 4267–4278. doi:10.1109/JSYST.2021.3108635

Kordestani, M., and Saif, M. (2021). Observer-based attack detection and mitigation for cyberphysical systems: A review. *IEEE Syst. Man. Cybern. Mag.* 7, 35–60. doi:10.1109/msmc.2020.3049092

Larkin, R. D., Wagner, T. J., and Mullins, B. E. "Securing photovoltaic system deployments with data diodes," in Proceedings of the Conference Record of the IEEE Photovoltaic Specialists Conference, Calgary, AB, Canada, June 2020. doi:10.1109/PVSC45281.2020.9300863

Li, B., Lu, R., and Xiao, G. "HMM-based fast detection of false data injections in advanced metering infrastructure," in Proceedings of the 2017 IEEE Global Communications Conference, Singapore, December 2017. doi:10.1109/GLOCOM.2017.8254498

Li, F., Li, Q., Zhang, J., Kou, J., Ye, J., Song, W. Z., et al. (2021). Detection and diagnosis of data integrity attacks in solar farms based on multilayer long short-term memory network. *IEEE Trans. Power Electron* 36, 2495–2498. doi:10.1109/TPEL.2020.3017935

Li, Q., Li, F., Zhang, J., Ye, J., Song, W., and Mantooth, A. "Data-driven cyberattack detection for photovoltaic (PV) systems through analyzing micro-PMU data," in Proceedings of the ECCE 2020 - IEEE Energy Conversion Congress and Exposition, Detroit, MI, USA, October 2020. doi:10.1109/ECCE44975.2020.9236274

Li, Q., Zhang, J., Ye, J., and Song, W. "Data-driven cyber-attack detection for photovoltaic systems: A transfer learning approach," in Proceedings of the Conference Proceedings - IEEE Applied Power Electronics Conference and Exposition - APEC, Houston, TX, USA, March 2022. doi:10.1109/APEC43599.2022.9773401

Liu, X., Shahidehpour, M., Cao, Y., Wu, L., Wei, W., and Liu, X. (2017). Microgrid risk analysis considering the impact of cyber attacks on solar PV and ESS control systems. *IEEE Trans. Smart Grid* 8, 1330–1339. doi:10.1109/TSG.2016.2622289

Lu, K. Di, Zeng, G. Q., Luo, X., Weng, J., Luo, W., and Wu, Y. (2021). Evolutionary deep Belief network for cyber-attack detection in industrial automation and control system. *IEEE Trans. Ind. Inf.* 17, 7618–7627. doi:10.1109/TII.2021.3053304

Ma, M. "Mitigating denial of service attacks with password puzzles," in Proceedings of the International Conference on Information Technology: Coding and Computing, Las Vegas, NV, USA, April 2005. doi:10.1109/itcc.2005.200

Miranda, A. W., and Goldsmith, S. (October 2017). Cyber-physical risk management for PV photovoltaic plants. in Proceedings - International Carnahan Conference on Security Technology Madrid, Spain, doi:10.1109/CCST.2017.8167813

Mustafa, A., Poudel, B., Bidram, A., and Modares, H. (2020). Detection and mitigation of data manipulation attacks in AC microgrids. *IEEE Trans. Smart Grid* 11, 2588–2603. doi:10.1109/TSG.2019.2958014

Patel, A., Roy, S., and Baldi, S. (2021). Wide-area damping control resilience towards cyber-attacks: A dynamic loop approach. *IEEE Trans. Smart Grid* 12, 3438–3447. doi:10.1109/TSG.2021.3055222

Peng, S., Liu, M., Zuo, K., Tan, W., and Deng, R. "Stealthy data integrity attacks against grid-tied photovoltaic systems," in Proc. - 2023 IEEE 6th Int. Conf. Ind. Cyber-Physical Syst. ICPS, Wuhan, China, May 2023, 1–7. doi:10.1109/ICPS58381.2023.10128033

Qiu, W., Sun, K., Li, K. J., Li, Y., Duan, J., and Zhu, K. (2023). Cyber-attack detection: modeling and roof-pv generation system defending. *IEEE Trans. Ind. Appl.* 59, 160–168. doi:10.1109/TIA.2022.3213629

Riggs, H., Tufail, S., Khan, M., Parvez, I., and Sarwat, A. I. "Detection of false data injection of PV production," in Proceedings of the IEEE Green Technologies Conference, Denver, CO, USA, April 2021. doi:10.1109/GreenTech48523.2021.00012

Shen, Y., Wang, L., Lau, J. P., and Liu, Z. "A robust control architecture for mitigating sensor and actuator attacks on PV converter," in Proceedings of the 2019 IEEE PES GTD Grand International Conference and Exposition Asia GTD Asia, Bangkok, Thailand, March 2019. doi:10.1109/GTDAsia.2019.8716017

Singh, V. K., and Govindarasu, M. (2021). A cyber-physical anomaly detection for wide-area protection using machine learning. *IEEE Trans. Smart Grid.* 12, 3514–3526. doi:10.1109/TSG.2021.3066316

Sourav, S., Biswas, P. P., Chen, B., and Mashima, D. "Detecting hidden attackers in photovoltaic systems using machine learning," in Proceedings of the 2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, SmartGridComm, Singapore, October 2022. doi:10.1109/SmartGridComm52983.2022.9960965

Tertytchny, G., Karbouj, H., Hadjidemetriou, L., Charalambous, C., Michael, M. K., Sazos, M., et al. "Demonstration of man in the middle attack on a commercial photovoltaic inverter providing ancillary services," in Proceedings of the 2020 IEEE CyberPELS, CyberPELS, Miami, FL, USA, October 2020. doi:10.1109/CyberPELS49534.2020.9311531

Taghezouit, B., Harrou, F., Sun, Y., Arab, A. H., and Larbes, C. (2021). A simple and effective detection strategy using double exponential scheme for photovoltaic systems monitoring. *Sol. Energy* 214, 337–354. doi:10.1016/j.solener.2020.10.086

Taghezouit, B., Harrou, F., Sun, Y., Arab, A. H., and Larbes, C. (2020). Multivariate statistical monitoring of photovoltaic plant operation. *Energy Convers. Manag.* 205, 112317. doi:10.1016/j.enconman.2019.112317

Tan, S., Guerrero, J. M., Xie, P., Han, R., and Vasquez, J. C. (2020). Brief survey on attack detection methods for cyber-physical systems. *IEEE Syst. J.* 14, 5329–5339. doi:10.1109/JSYST.2020.2991258

Tuyen, N. D., Quan, N. S., Linh, V. B., Van Tuyen, V., and Fujita, G. (2022). A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy. *IEEE Access* 10, 35846–35875. doi:10.1109/ACCESS.2022.3163551

Walker, A., Desai, J., Saleem, D., and Gunda, T. (2021). Cybersecurity in photovoltaic plant operations. Available at: www.nrel.gov/publications.

Wang, R., Ma, D., Li, M. J., Sun, Q., Zhang, H., and Wang, P. (2022a). Accurate current sharing and voltage regulation in hybrid wind/solar systems: an adaptive dynamic programming approach. *IEEE Trans. Consum. Electron* 68, 261–272. doi:10.1109/TCE.2022.3181105

Wang, R., Sun, Q., Zhang, P., Gui, Y., Qin, D., and Wang, P. (2020). Reduced-order transfer function model of the droop-controlled inverter via Jordan continued-fraction expansion. *IEEE Trans. Energy Convers.* 35, 1585–1595. doi:10.1109/TEC.2020.2980033

Wang, W., Harrou, F., Bouyeddou, B., Senouci, S. M., and Sun, Y. (2022b). Cyber-attacks detection in industrial systems using artificial intelligence-driven methods. *Int. J. Crit. Infrastruct. Prot.* 38, 100542. doi:10.1016/j.ijcip.2022.100542

Wei, L., Gao, D., and Luo, C. "False data injection attacks detection with deep Belief networks in smart grid," in Proceedings of the 2018 Chinese Automation Congress, CAC, Xi'an, China, November 2019. doi:10.1109/CAC.2018.8623514

Ye, J., Giani, A., Elasser, A., Mazumder, S. K., Farnell, C., Mantooth, H. A., et al. (2022). A review of cyber-physical security for photovoltaic systems. *IEEE J. Emerg. Sel. Top. Power Electron.* 10, 4879–4901. doi:10.1109/JESTPE.2021.3111728

Zegeye, W. K., Dean, R. A., and Moazzami, F. (2019). Multi-layer hidden Markov model based intrusion detection system. *Mach. Learn. Knowl. Extr.* 1, 265–286. doi:10.3390/make1010017

Zetter, K. (2016). Inside the cunning, unprecedented hack of Ukraine's power grid. Available at: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (Accessed August 8, 2023).

Zhang, J., Guo, L., and Ye, J. (2022). Cyber-attack detection for photovoltaic farms based on power-electronics-enabled harmonic state space modeling. *IEEE Trans. Smart Grid.* 13, 3929–3942. doi:10.1109/TSG.2021.3121009

Zhao, L., Li, J., Li, Q., and Li, F. (2022). A federated learning framework for detecting false data injection attacks in solar farms. *IEEE Trans. Power Electron* 37, 2496–2501. doi:10.1109/TPEL.2021.3114671

Zhong, X., Jayawardene, I., Venayagamoorthy, G. K., and Brooks, R. (2017). Denial of service attack on tie-line bias control in a power system with PV plant. *IEEE Trans. Emerg. Top. Comput. Intell.* 1, 375–390. doi:10.1109/TETCI.2017.2739838

Zhou, Q., Shahidehpour, M., Alabdulwahab, A., Abusorrah, A., Che, L., and Liu, X. (2021). Cross-layer distributed control strategy for cyber resilient microgrids. *IEEE Trans. Smart Grid* 12, 3705–3717. doi:10.1109/TSG.2021.3069331