International Journal of Applied Power Engineering (IJAPE)
Vol. 14, No. 4, December 2025, pp. 1044∼1057
ISSN: 2252-8792, DOI: 10.11591/ijape.v14.i4.pp1044-1057

Systematic literature review on cyber-attacks and cyber defense strategies in smart grids

Anass Naqqad, Abdellah Boulal, Rachid Habachi
Laboratory of Engineering, Industrial Management and Innovation, Faculty of Sciences and Technology, Hassan 1st University, Settat, Morocco

Article Info

Article history:

Received Sep 24, 2024
Revised Aug 13, 2025
Accepted Oct 16, 2025

Keywords:

Cyber-attack
Cyber defense
Cyber security
Smart grid
Systematic literature review

ABSTRACT

The smart grid is an advanced evolution of the traditional electrical power grid, developed to meet the increasing energy demands and requirements of the 21st century by incorporating digital technologies and data management systems to improve efficiency and reliability. Unlike conventional grids, the smart grid relies on a network of interconnected digital devices, sensors, and computerized controls that enable real-time monitoring and management of electricity distribution across vast geographic areas. However, the growing dependence on digital technologies also brings heightened cyber security concerns, since their integration can expose the grid to an increased risk of malicious intrusions. This systematic literature review investigates the nature and scope of cyber-attacks and cyber defense strategies in smart grids, which are critical to modern energy infrastructure. Following established research guidelines, this review rigorously examines existing studies by focusing on peer-reviewed articles and conference papers to understand the range of cyber security threats and defense mechanisms that smart grids face. The review uses a structured methodology to identify, evaluate, and synthesize key findings, revealing trends and gaps in current knowledge about smart grid security. The outcomes of this analysis offer valuable clarity on the specific weaknesses and operational challenges that affect smart grid infrastructures, contributing to the ongoing efforts to enhance cyber security measures and guide future research in this vital field.

Corresponding Author:

Anass Naqqad
Laboratory of Engineering, Industrial Management and Innovation, Faculty of Sciences and Technology
Hassan 1st University
PO Box 577, Settat, Morocco
Email: a.naqqad.doc@uhp.ac.ma

1. INTRODUCTION

Smart grids face increasing cyber threats due to their growing digital complexity. The integration of advanced communication, automation, and data analytics has expanded their attack surface, making them vulnerable to sophisticated threats that can compromise control, availability, integrity, and confidentiality. While numerous studies address individual threats, recent literature lacks a structured synthesis of attack and defense strategies using the CAIC framework, especially for emerging trends between 2020 and 2024. This paper addresses that gap by categorizing cyber-attacks through the CAIC model and synthesizing state-of-the-art defense methods to inform future research and policy.

Smart grids represent a transformative step in modern energy management, integrating information and communication technologies with traditional power systems to optimize electricity production, distribution, and consumption. This innovation enables better management of electricity demand, integration of renewable energy sources, and efficient response to real-time changes in supply and demand. As the grid's complexity increases with the inclusion of decentralized power systems and variable renewable energy sources, smart grids offer the flexibility needed to maintain stability and reliability. The International Energy Agency notes that by 2030, the energy landscape will undergo significant changes due to current policy settings, emphasizing the importance of adaptive smart grid solutions to accommodate these shifts and ensure sustainable energy management [1].

Smart grids are advanced electricity networks that integrate the actions of generators, consumers, and prosumers to efficiently deliver sustainable and secure electricity [2]. Using digital communication systems, smart grids stand apart from conventional power grids, allowing two-way data exchange between energy providers and end-users through smart meters, sensors, and automated controls. This allows for real-time management of electricity supply and demand and supports distributed energy resources like wind and solar power. According to the US National Institute of Standards and Technology (NIST), a smart grid comprises seven logical domains: bulk generation, transmission, distribution, customer, markets, service provider, and operations [3]. Together, these domains enhance grid efficiency, reliability, and sustainability.

The development of smart grids is driven by the demand for reliable, sustainable energy solutions. As the global energy landscape shifts toward decarbonization and decentralization, traditional grids struggle to manage challenges like integrating renewable energy and handling peak loads. Smart grids address these issues with real-time monitoring and enhanced stability, but their increased complexity also makes them more vulnerable to cyber threats. Communication technologies and consumer data are particularly exposed, posing significant challenges to broader deployment and integration [4].

Cybersecurity challenges in smart grids encompass a wide range of threats, from common data breaches and ransomware attacks to more sophisticated methods such as distributed denial of service (DDoS) attacks, advanced persistent threats (APT), phishing, spyware, rootkits, ransomware, and SQL injection [5]. These attacks, which can target the grid's control systems and data integrity, present significant risks that, if not properly managed, can lead to severe disruptions, financial losses, and safety concerns. To combat these diverse threats, advanced techniques like machine learning, anomaly detection, and multi-stage intrusion detection systems are increasingly being employed [6]. Moreover, deep learning approaches have also shown great potential in improving threat detection and enhancing response capabilities within smart grid environments [7].

While several reviews have explored cybersecurity in smart grids, many span broad timeframes without emphasizing recent advancements [8]. Moreover, they often concentrate on a narrow set of well-known attack types, overlooking the broader landscape of potential threats [9]. In contrast, this paper presents a timely and systematic review that employs the CAIC framework to categorize attacks—explicitly linking each threat to its corresponding impact area and covering a wider range of attack vectors.

This paper presents a systematic and comprehensive review of research on cyber-attacks and defense strategies in smart grids from 2020 to 2024. It synthesizes findings from various studies to highlight the current state of cybersecurity measures, systematically identifies gaps in existing research, and proposes future directions for enhancing the resilience of smart grids against evolving cyber threats. By examining different types of cyber threats, their impacts, and potential mitigation strategies, this systematic review aims to contribute to the development of more robust cybersecurity frameworks capable of protecting smart grids from emerging challenges.

The paper is structured as follows: Section 2 outlines the methodology employed for the systematic literature review. Section 3 presents the results, followed by a discussion. Finally, section 4 provides the conclusions.

2. METHOD

2.1. Search strategy

This systematic literature review (SLR) adopts a well-defined, replicable process, drawing on Kitchenham's methodology for evidence-based software engineering [10], [11]. Kitchenham's framework was chosen for its methodological rigor and suitability for multidisciplinary, technology-driven domains such as smart grid cybersecurity—where reproducibility, traceability, and transparency are critical.

The need for this review stems from notable gaps in the existing literature. While several studies have explored cybersecurity in smart grids, no current review provides a comprehensive synthesis of recent developments alongside a broad categorization of attack types and their associated impacts. Many existing reviews span long timeframes without emphasizing emerging threats, or they focus narrowly on a limited set of well-known attack vectors.

Accordingly, this review explicitly defines its scope to focus on identifying and analyzing cyber-attacks targeting smart grids, along with the corresponding mitigation strategies employed to defend these systems. To guide the review process, we formulated two research questions: i) What are the predominant cyber-attacks discussed in the current literature related to smart grids? and ii) How are these attacks addressed in existing studies, and what cyber defense strategies are proposed?

A comprehensive search strategy was adopted to locate relevant literature. This involved using reputable databases known for publishing scholarly articles on smart grids and cybersecurity. The primary digital libraries selected for this review are: i) IEEE Xplore, ii) Web of Science, and iii) ACM Digital Library. These leading digital libraries were chosen for their extensive coverage of peer-reviewed works in engineering, computer science, and cybersecurity. IEEE Xplore offers the most comprehensive smart grid research, Web of Science ensures multidisciplinary indexing, and ACM Digital Library provides strong coverage of computing and network security.

To refine the search process, specific keywords and Boolean operators were used, with ”attack” and ”smart grid” selected as the main search terms. These keywords were chosen to focus on offensive aspects of cybersecurity, ensuring that retrieved studies addressed direct threats rather than only general security measures. Boolean operators and title-specific searches were applied to increase precision and reduce irrelevant results.

– IEEE Xplore Search Query:
  Boolean/Phrase: `("Document Title": attack)` AND `("Document Title": smart grid)`
  Refined by content type: conferences and journals.
– Web of Science Search Query:
  Boolean/Phrase: `(TI=(attack) AND TI=(smart grid)) AND ((DT=(Article)) OR DT=(Proceedings Paper) OR DT=(Review Article))`
– ACM Digital Library Search Query:
  Boolean/Phrase: `[Title: attack] AND [Title: smart grid]`
  Refined by publication type: proceedings and journals.

2.2. Inclusion and exclusion criteria

To ensure that only pertinent and high-quality studies were included in the review, clear inclusion and exclusion criteria were defined. These criteria guided the filtering of results obtained from the search pro- cess and ensured consistency in study selection. The criteria are summarized below:

– Inclusion criteria: i) studies directly related to smart grid cyber security, ii) publication dates ranging from January 1, 2020, to March 31, 2024, and iii) publications in English.
– Exclusion criteria: i) duplicate publications and ii) articles focusing on cyber security aspects of related fields like IoT or EVs without a direct emphasis on smart grids.

2.3. Screening process

The screening was carried out in two stages. Initially, titles and abstracts were reviewed to filter out studies that did not meet the predefined inclusion and exclusion criteria. Subsequently, a comprehensive full-text evaluation was performed to determine study quality and collect information relevant to the research questions. Figure 1 illustrates the study selection process following the PRISMA guidelines.

2.4. Quality assessment

To maintain the validity and reliability of our findings, we applied a structured quality assessment to all included studies. This process ensured that only technically sound, well-documented, and relevant research contributed to the final synthesis. The evaluation relied on four binary criteria, selected to cover methodological clarity, practical validation, measurable outcomes, and critical analysis.

These criteria were assessed independently by two reviewers to reduce bias, with disagreements resolved through discussion until consensus was reached. Each criterion was scored as either *met* (1) or *not met*

(0), and a study had to achieve a minimum score of 3/4 to be retained. This threshold strikes a balance between maintaining a high standard and avoiding the exclusion of potentially valuable insights. Table 1 presents the criteria alongside their underlying rationale. This multi-step evaluation ensured consistency, transparency, and scalability across all reviewed papers, thereby increasing the robustness of the final synthesis.

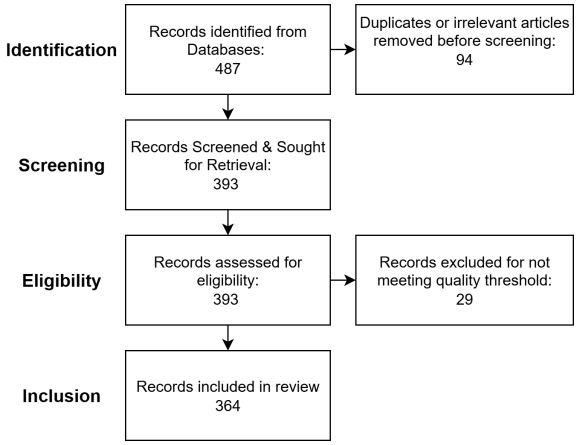

Figure 1. PRISMA flow diagram of the study selection process

Table 1. Quality assessment criteria and their rationale

No.	Criterion	Rationale
1	The method is clearly described and reproducible.	Ensures transparency and enables replication of findings by other researchers.
2	The study includes a simulation, real-world system, or experimental validation.	Confirms that results are based on practical implementation rather than purely theoretical analysis.
3	The results section presents measurable outputs or evaluation metrics.	Provides quantifiable evidence to support claims and allow performance comparison across studies.
4	The findings are critically discussed and compared to prior work.	Demonstrates awareness of existing literature and positions the study within the broader research context.

3. RESULTS AND DISCUSSION

We first conducted a comprehensive search to identify all research papers related to the cybersecurity of smart grids. This process yielded a total of 487 articles. The search was carried out across three major databases: Web of Science, IEEE Xplore, and the ACM Digital Library. Table 2 presents the annual distribution of these initial papers before applying any exclusion criteria. This includes all retrieved records regardless of quality, duplication, or relevance.

Following an initial screening based on titles, abstracts, and predefined inclusion/exclusion criteria, 94 papers were excluded due to duplication or lack of relevance to smart grid cyber security. In the second phase, the remaining 393 articles were examined in full to evaluate their quality. Based on the four-point evaluation criteria, 29 papers failed to meet the minimum quality threshold and were removed. Consequently, 364 high-quality papers were retained for final synthesis and analysis. Our systematic review identified several distinct research streams within the domain of smart grid cybersecurity. These streams, summarized in Figure 2, illustrate the thematic areas most frequently addressed by the reviewed studies, providing an overview of where current research efforts are concentrated. Our findings indicate a stronger emphasis on enhancing cyber defense mechanisms rather than developing cyber-attack strategies. Specifically, researchers tend to focus on developing new mitigation techniques for the most critical threats facing smart grids, instead of adopting an offensive approach, similar to that of malicious actors, by formulating new attack strategies. Furthermore, several studies propose novel simulation frameworks that allow researchers to analyze and simulate potential cyber-attacks, enabling them to better anticipate future threats, thereby strengthening defense mechanisms and improving overall risk management. Additionally, other studies emphasize the importance of distinguishing system faults from cyber-attacks, while others focus on comprehensive risk management strategies. The papers were also categorized by research method analytical, simulation, or literature review as shown in Figure 3. This distribution reveals methodological preferences within the field and helps identify underexplored approaches.

Table 2. Annual distribution of retrieved papers by database

Year	Web of Science	IEEE	ACM library	Total count
2020	41	52	4	97
2021	44	50	8	102
2022	61	61	3	125
2023	52	65	5	122
2024	18	20	3	41

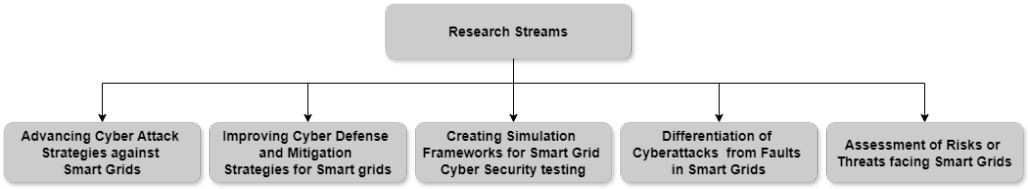

Figure 2. Research streams identified in the scope of this systematic literature review

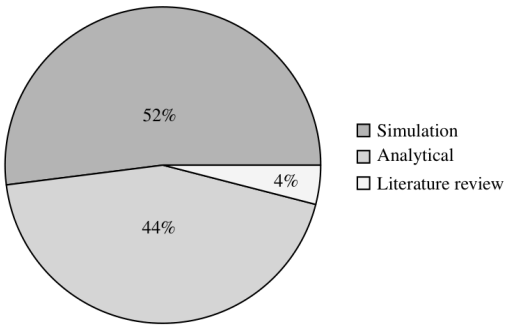

Figure 3. Classification of publications by research method

The analysis of research methods across the reviewed papers shows a clear preference for simulation, analytical approaches, or a combination of both, with fewer studies dedicated to literature reviews, especially systematic ones. This suggests an emphasis on developing and testing specific models or solutions rather than synthesizing existing knowledge. Expanding the number of systematic literature reviews could offer a broader view of the research landscape, highlight gaps, and guide future studies toward more innovative and effective strategies. In addition, several studies combine multiple methodologies, such as simulation validated with analytical models, to achieve more robust and generalizable findings. This trend reflects an increasing effort to balance technical rigor with practical applicability, an approach that can be particularly valuable when addressing the multifaceted security challenges of smart grids.

In information technology (IT), the primary security focus is on the CIA triad (confidentiality, integrity, availability). However, in operational technology (OT), such as smart grids, the emphasis shifts to the CAIC model (control, availability, integrity, confidentiality), as shown in Figure 4. The cyber-attacks identified from the reviewed literature were categorized based on their impact on these four CAIC dimensions - control, availability, integrity, and confidentiality - providing a structured framework for understanding how each threat affects different aspects of smart grid security. In IT systems, confidentiality is traditionally prioritized, but in operational technology (OT) environments like smart grids, control and availability take precedence due to their critical role in ensuring operational continuity and safety. The CAIC model—control, availability, integrity, and confidentiality—captures this shift. Control ensures only authorized users can influence system behavior; availability minimizes disruption by guaranteeing timely access to services and data; integrity preserves accuracy and consistency of information; and confidentiality safeguards sensitive data from unauthorized access.

This extended model guided the classification of cyber-attacks in this study. Table 3 presents each attack type alongside its affected CAIC dimension(s), illustrating how specific threats compromise various facets of smart grid security. Integrity appears as the most frequently targeted objective, particularly in attacks like FDIA and topology manipulation. Availability is commonly disrupted by DoS and load-altering attacks.

Control is threatened by remote access exploits, resonance manipulation, and Sybil attacks. Meanwhile, confidentiality is often breached through deceptive means such as social engineering, MitM attacks, and data mining.

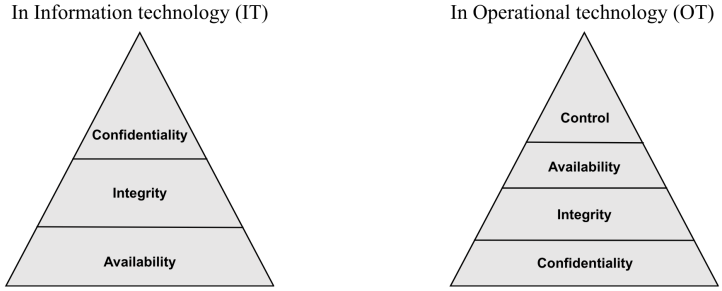

Figure 4. Security priorities in IT and OT

Table 3. Cyber-attacks on smart grids and their impact areas

Attack type	Impact area	Description
False data injection attacks (FDIA) [12]	Integrity	Alters data to mislead systems or users.
Denial of service (DoS) [13]	Availability	Overwhelms a system to prevent legitimate access.
Distributed denial of service (DDoS) [14]	Availability	Overwhelms a system or network with a flood of internet traffic from multiple sources.
Replay attacks [15]	Confidentiality, integrity	Retransmits valid data to repeat or delay transactions.
Adversarial attacks [16]	Integrity, control	Manipulates inputs to machine learning models to produce incorrect outputs.
Cyber-physical attacks [17]	Availability, integrity, control	Targets both cyber and physical components, affecting critical infrastructure.
ARP cache poisoning [18]	Confidentiality, integrity	Misleads devices by associating incorrect MAC addresses to intercept or alter traffic.
Remote access [19]	Confidentiality, control	Exploitation of remote access tools to gain unauthorized control over systems.
Supply chain attacks [20]	Confidentiality, integrity, control	Uses components or software provided by third parties to infiltrate a target organization.
Internal attacks [21]	Confidentiality, integrity, availability, control	Perpetrated by insiders with legitimate access to the system or network.
Social engineering [22], [23]	Confidentiality, control	Manipulates human behavior to obtain unauthorized information or system access.
Malware [24]	Confidentiality, availability, integrity, control	Deploys malicious software to disrupt, steal data, or gain unauthorized control.
Man-in-the-Middle (MitM) [25]	Confidentiality, integrity	Captures and possibly modifies the exchange of information between two communicating entities.
GPS spoofing [26]	Integrity	Falsifies GPS signals to mislead location-based services.
Dynamic load altering attack [27]	Availability, integrity	Manipulates load conditions to disrupt power system stability.
Data mining [28]	Confidentiality	Analyzes large datasets to extract sensitive or valuable information.
Coordinated cyber-physical attack [29]	Availability, integrity, control	Simultaneous or synchronized attacks targeting both cyber and physical layers.
Topology attack [30]	Integrity, control	Targets the system's physical or logical structure by manipulating the network's layout or configuration.
Cascading failure attack [31]	Availability, control	Initiates a sequence of failures that affect interconnected components.
Wormhole attack [32]	Confidentiality, integrity	Creates a tunnel between malicious nodes to disrupt network communication.
Sybil attack [33]	Integrity, control	Creates multiple fake identities to manipulate network protocols.
Resonance attacks (ResA) [34]	Availability, control	Targets resonance resources to manipulate or modify power plant inputs based on resonance reference.
Time synchronization attacks (TSA) [35]	Integrity, availability	target timing data in smart grids, causing false alarms and communication disruptions, potentially leading to cascading faults.

Notably, sophisticated threats—such as cyber-physical, internal, and supply chain attacks—often span multiple CAIC domains, exploiting both technical and human vulnerabilities. While the literature addresses a broad range of attack types across all CAIC domains, special attention should be given to threats targeting control. Because control governs system actions and real-time decision pathways, breaches in this area pose the most direct risks to physical safety and operational continuity. Prioritizing detection and mitigation strategies for control-focused attacks is therefore essential for ensuring smart grid resilience.

Our research highlights that false data injection attacks (FDIAs) have remained a major threat to smart grids over the past four years. Alongside distributed denial of service (DDoS) attacks, FDIAs require focused defense strategies. Moreover, there is a growing trend toward adversarial attacks targeting machine learning-based defenses, underscoring the need for adaptive countermeasures. Our analysis also revealed that coordinated cyber-physical attacks, malware, internal threats, and supply chain attacks have the most significant impact when evaluated through the CAIC framework. These observations are reflected in the focus areas of the most cited papers identified in this review, as presented in Table 4.

Table 4. Anchor paper bibliography

Article title	Authors	Citations	Findings
Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach [12]	Zhang, Ying; Wang, Jianhui; Chen, Bo	222	Uses minimal labeled data and generative models for FDIA detection in smart grids.
Detection of false data injection attacks in smart grid: A secure federated deep learning approach [36]	Li, Yang; Wei, Xinhao; Li, Yuanzheng; Dong, Zhaoyang; Shahidehpour, Mohammad	189	Uses federated learning and transformer-based models with privacy-preserving mechanisms for FDIA detection.
Smart grid cyber-physical attack and defense: A review [37]	Zhang, Hang; Liu, Bo; Wu, Hongyu	181	Surveys cyber-physical attack models and proposes a new taxonomy with recent defense strategies.
Extremely randomized trees-based scheme for stealthy cyber-attack detection in smart grid networks [38]	Camana Acosta, Mario R.; Ahmed, Saeed; Garcia, Carla E.; Koo, Insoo	152	Combines KPCA and extra-trees algorithm to detect stealthy cyber-attacks.
Detection of false data injection attacks in smart grids based on graph signal processing [39]	Drayer, Elisabeth; Routtenberg, Tirza	141	Applies graph signal processing and filters to detect FDIA in AC systems.

To address the various cyber threats identified earlier, a range of cyber defense methods have been identified in the literature to enhance security and resilience against potential attacks for each type of threat:

- Machine learning and deep learning techniques: AI-based methods have become central to cybersecurity solutions in smart grids due to their adaptability and pattern recognition capabilities. One study introduces a data-driven machine learning approach that identifies stealthy false data injection attacks (FDIAs) on state estimation through the application of ensemble learning methods. This approach employs both supervised and unsupervised classifiers, showing that unsupervised ensemble models outperform individual classifiers in detecting stealthy FDIAs [40]. A model focuses on detecting DoS attacks by using PCA for dimensionality reduction and SVM for anomaly detection, outperforming other classifiers on the KDD99 dataset [41]. Additionally, hybrid machine learning models in [24] evaluate supervised learning techniques with various boosting and feature selection methods to enhance FDIA detection in smart grids.
- Intrusion detection and anomaly detection: As smart grids increasingly integrate with communication systems, the detection of irregular behavior becomes a critical line of defense. Sriranjani *et al.* [42] proposed a machine learning-based scheme that effectively detects replay attacks by analyzing real-time sensor data using fine gaussian support vector machine to classify data as either normal or malicious, demonstrating high accuracy in replay attack detection in smart grids. Additionally, Jin *et al.* [43] introduced an anomaly detection framework based on an attack-chain knowledge graph and a multi-layer detection system, improving the detection of unknown and multi-step attacks in power grid networks, particularly in internal and external interactions of smart grids.
- State estimation and control strategies: Effective control and accurate state estimation are foundational to grid security and resilience. For instance, techniques such as physical watermarking, which rely on set-theoretic model predictive control, are instrumental in actively detecting replay attacks while maintaining system stability [15]. Although Kalman-filter-based detectors are widely used for identifying FDIAs, they remain susceptible to noise-exploitation tactics, highlighting the need for more resilient solutions [44].

More advanced approaches, like fourier singular values-based detection, improve FDIA identification in AC systems by utilizing refined state estimation techniques to uncover anomalies [45]. Additionally, strategic PMU placement enhances detection capabilities by boosting state estimation precision and mitigating coordinated FDIAs, especially in environments with limited resources [46]. Furthermore, resonance attacks, which exploit the rate of change in frequency to destabilize power systems, demand specific countermeasures. A detection and mitigation control scheme employing an artificial neural network (ANN) observer-based sliding mode controller (SMC) has been shown to efficiently detect and neutralize these attacks by stabilizing frequency oscillations and minimizing chattering, as demonstrated through simulations [34].

- Cryptography and privacy: In a data-centric environment like the smart grid, securing communication and maintaining user privacy are essential. Wang *et al.* [21] proposed a lightweight privacy-preserving data aggregation protocol that enhances security by aggregating electricity consumption data while resisting internal attacks, such as collusion from data centers or shared information attacks. Additionally, Hafeez *et al.* [47] developed an enhanced differential privacy model (E-DPNCT), which provides robust protection against collusion attacks in smart grids by using a split noise cancellation protocol with multiple master smart meters, ensuring both privacy and accurate billing and load monitoring.
- Risk management and mitigation: Proactively quantifying and managing risks allows operators to prepare for and respond to evolving cyber threats more effectively. Rios *et al.* [48] proposed a continuous quantitative risk management methodology utilizing attack defense trees to provide a comprehensive assessment of cyber risks in smart grids. This approach supports informed decision-making by continuously evaluating risks across various attack and defense scenarios and optimizing security strategies for risk minimization. Additionally, another study employs Bayesian networks to assess the risk of cyber-physical attacks, such as manipulating circuit breakers in smart grids. By combining vulnerabilities in the cyber domain with transient stability analysis in the physical domain, the model provides a framework for quantifying risks and enhancing grid resilience [49].
- Optimization and game theory: Strategic modeling through optimization and game theory offers a structured way to allocate defensive resources and anticipate adversarial behavior. Shan and Zhuang [50] presented a model that simulates attacks and defenses at three levels—power plants, transmission, and distribution—helping to identify equilibrium strategies that optimize defense efforts based on attack success probabilities. Additionally, another study applies game theory to optimize defense resources against false data injection attacks on energy management systems, offering effective monitoring strategies and revealing Nash equilibrium solutions for mitigating these attacks [51].

To consolidate the insights from our review, we synthesized the most prominent attack types identified in the literature, mapping them to their corresponding CAIC impact areas and the defense mechanisms most frequently employed against them. This synthesis serves as a bridge between the threat landscape and the mitigation strategies, enabling a clearer understanding of how research efforts are currently distributed across different attack categories. While some threats, such as FDIAs and DoS/DDoS, benefit from well-developed and diverse countermeasures, others—particularly adversarial ML attacks and supply chain threats—remain less extensively addressed, underscoring the uneven maturity of defense approaches across the spectrum of smart grid cybersecurity challenges. To complement the synthesis in Table 5, Figure 5 visualizes the mapping between the identified attack types and the CAIC security dimensions:

While the literature demonstrates solid technical progress—particularly in the use of machine learning, deep learning, and anomaly detection—the strong emphasis on these approaches reveals a narrowing of focus in the field. A clear trend is the dominance of research on false data injection attacks (FDIA), which remain the most studied threat, alongside sustained interest in distributed denial of service (DDoS) attacks. More recently, there has been a notable rise in adversarial machine learning, where attack strategies are designed to evade AI-based detection models, signaling a shift toward more sophisticated threat scenarios. Simulation-based methodologies, often validated with analytical models, also dominate the research landscape, reflecting a preference for controlled experimentation over large-scale real-world deployments.

However, this concentration comes at the expense of several important areas. Cryptographic approaches, such as blockchain-enabled data integrity, and strategic security models based on game theory—both critical for long-term resilience—receive comparatively limited attention. Similarly, emerging domains like blockchain vulnerabilities, post-quantum cryptography, and systematic threat intelligence frameworks are rarely addressed despite their growing relevance to future-proof security. Offensive research,

including red-teaming exercises and simulated adversarial campaigns, is also underrepresented, leaving a gap in anticipatory defense strategies that more closely mirror the behavior of real-world attackers.

In addition, system-level challenges stemming from the increasing decentralization and complexity of smart grids are insufficiently explored. For instance, the rapid integration of cloud infrastructure introduces new attack surfaces, yet few studies propose security models tailored to hybrid or multi-cloud smart grid environments. There is also a lack of focus on secure communication protocol design, particularly protocols that simultaneously address confidentiality, integrity, and accountability. These gaps highlight the need for a broader and more multidisciplinary research agenda that complements the current defense-oriented approach with forward-looking strategies capable of addressing both present and emerging threats.

Table 5. Attack types and common defense methods

Attack Type	Common defense methods
False data injection attacks (FDIA)	State estimation validation, machine learning anomaly detection, PMU placement optimization
Denial of service (DoS/DDoS)	Network segmentation, traffic filtering, anomaly detection
Adversarial ML attacks	Robust model training, input preprocessing, adversarial detection frameworks
Supply chain attacks	Component validation, blockchain-based provenance, secure firmware updates
Replay attacks	Time-stamping, watermarking, encryption
Cyber-physical attacks	Physical redundancy, intrusion detection, coordinated incident response

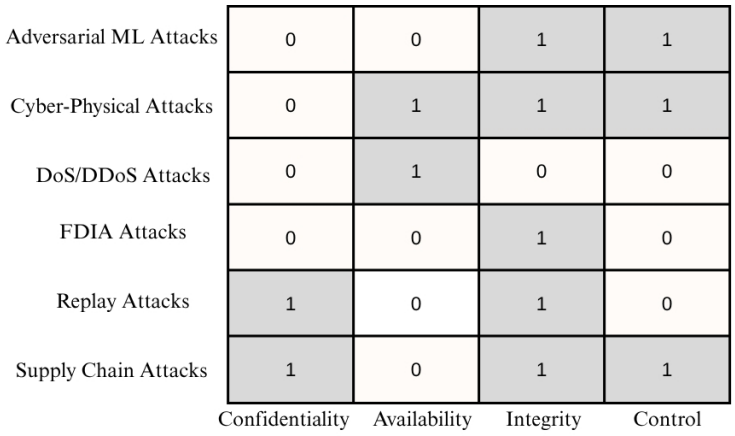

Figure 5. CAIC mapping of major attack types based on reviewed literature

To further advance research on smart grid security, it is essential to explore these new directions to address emerging challenges and gaps in current strategies:

– Focusing more on cyber attack development for smart grids: While much of the current research focuses on developing cyber defense strategies, there is a critical need to place greater emphasis on creating and understanding cyber attack methods in smart grids. Developing more sophisticated simulated attack models and conducting red team exercises can provide deeper insights into potential vulnerabilities and weaknesses in smart grid systems. By focusing more on the development of innovative attack methodologies, researchers can better anticipate threats and improve defensive mechanisms, ultimately leading to more robust and comprehensive cybersecurity solutions.
– Focusing on threat intelligence: Although threat intelligence plays a vital role in anticipating cyber threats by delivering actionable insights into emerging attack vectors and tactics, it remains underrepresented in existing literature. There is a need for more research into threat intelligence frameworks specific to smart grids. Collaborative threat intelligence sharing platforms among utilities, governments, and private sectors can enhance situational awareness and coordinated defense strategies, making smart grids more resilient. Integrating threat intelligence with AI, blockchain, and advanced classification techniques can help maintain a comprehensive and adaptive defense posture.
– Leveraging generative AI for cyber defense: Generative AI (Gen AI) offers significant potential for both enhancing cyber defense and crafting sophisticated cyber attacks. In cyber defense, Gen AI can improve smart grid security by identifying anomalies and predicting attacks. For instance, using improved wasserstein

generative adversarial networks (WGAN) has proven effective in recovering from data integrity attacks in power systems [52]. Conversely, in adversarial machine learning (AML), Generative AI can be employed to generate evasion attacks that modify input data to mislead machine learning models, as demonstrated in a study where such attacks markedly reduced the detection accuracy of security classifiers for smart meters [53].Expanding research in this area could unlock new opportunities for proactive and adaptive cyber defense strategies in smart grids.

- Improving threat classification: Differentiating between cyber attacks and system faults is crucial for smart grid defense. Advanced machine learning, such as deep learning, enhances the accuracy of distinguishing these incidents for targeted responses. For instance, researchers have developed a discrimination algorithm that differentiates between electrical faults and cyber attacks, aiding in creating intelligent defense measures against grid mal-operations [54]. Adaptive systems that evolve with new attack patterns and anomalies are essential for robust defense mechanisms.
- Broadening cyber defense focus beyond false data injection attacks: While much of the current research has centered on defending against false data injection attacks (FDIA), there is a growing need to shift attention to other sophisticated cyber threats. Adversarial attacks that manipulate machine learning models and side-channel attacks that exploit information leakage are emerging as significant challenges [55]. Addressing these threats requires robust, adaptive algorithms and layered defenses that protect both software and hardware, ensuring comprehensive protection against a broader range of cyber-attack vectors.
- Enhancing cyber awareness: Human error remains a major cybersecurity weakness, compounded by the limited cyber awareness present in the power electronics community [56]. Strengthening cyber awareness through targeted training helps stakeholders recognize threats like phishing and social engineering, empowering them to act as effective defenders and reducing risks. Addressing this gap in cyber awareness is crucial for ensuring that professionals in power electronics can effectively identify and respond to potential cyber threats.
- Enhancing identity and access management: Advanced IAM is essential for securing smart grids against unauthorized access and insider threats. Recent research highlights the use of physical unclonable functions (PUFs) and blockchain to improve authentication and access control [57], [58]. Integrating decentralized identity management with these technologies can enhance security against both cyber and physical attacks, ensuring secure data exchange and system integrity. Future IAM solutions should focus on multi-factor authentication, real-time access monitoring, and tamper-resistant frameworks to address the complex security challenges in smart grids.
- Leveraging blockchain for enhanced security: Blockchain technology can provide significant benefits in securing smart grids by ensuring data integrity, transparency, and tamper resistance. It can be used for secure data exchange, decentralized identity management, and enhancing the trustworthiness of transactions across the grid. The potential of blockchain to address key security, privacy, and trust issues in smart grids makes it a valuable addition to smart grid security frameworks [59]. Integrating blockchain with smart grid systems can create a distributed and immutable ledger, preventing data tampering and enhancing overall system resilience against cyber-attacks.
- Developing quantum-resistant cryptography: As quantum computing advances, current cryptographic methods could become vulnerable. Developing quantum-resistant cryptographic algorithms specifically designed for smart grids is critical to safeguarding data integrity and confidentiality in a post-quantum era. Additionally, the use of quantum computers for encryption purposes can be highly effective for enhancing data security [60]. Future research should prioritize developing algorithms that combine efficiency with resilience against quantum-based attacks, thereby ensuring long-term security for smart grid systems.
- Enhancing cloud computing security in smart grids: Cloud computing is becoming increasingly important for smart grid systems due to its ability to enhance scalability, flexibility, and efficiency. However, this integration introduces significant cybersecurity challenges [61]. The use of cloud environments in smart grids increases the risk of cyber-attacks (CAs) by exposing sensitive data and critical infrastructure to potential breaches. Therefore, more research is needed to develop robust security measures tailored specifically for cloud-based smart grid systems.
- Development of secure communication protocols: Focusing on creating new protocols that address confidentiality, privacy, integrity, and accountability is crucial, as current protocols primarily emphasize connectivity. Developing secure communication protocols can help maintain the integrity and security of data transmission within smart grids.

– Adopting advanced risk management approaches: Given the complexity of smart grids, which represent a paradigm shift over traditional power grids, there is a need for developing unified frameworks that incorporate probabilistic models, risk breakdown structures, and advanced threat modeling to manage the intricate risks inherent in smart grids. Such frameworks should provide a holistic view that encompasses safety, security, and privacy risks across multiple layers and domains, as suggested by SGAM and NIST [62]. Addressing the unique interactions, protocols, and devices of the smart grid infrastructure, these approaches enable more comprehensive risk assessment, planning, and response to potential cyber threats, while also incorporating integrated security mechanisms for field devices, secure access control, and secure communication protocols.
– Increasing co-simulations and datasets for ML development: To advance AI and machine learning capabilities in smart grid security, there is a need for more realistic simulations of smart grid environments, particularly co-simulations, and the development of large, high-quality datasets. These datasets should represent diverse scenarios and attack types to train more robust and accurate ML models, enhancing their effectiveness in detecting, classifying, and mitigating cyber threats.

4. CONCLUSION

This systematic literature review maps the evolving landscape of cyber-attacks and defense mechanisms in smart grids, revealing both technological progress and persistent gaps. As the digitalization of smart grids accelerates, they face heightened risks from sophisticated threats such as false data injection attacks (FDIAs), distributed denial of service (DDoS) attacks, and adversarial machine learning exploits. While advancements in machine learning, anomaly detection, and state estimation have strengthened defensive capabilities, the field remains disproportionately focused on reactive measures. Critical areas—such as proactive attack modeling, realistic simulation environments, and validation using real-world datasets—remain underexplored. The analysis underscores the urgency of diversifying research to include generative AI for cyber offense–defense co-evolution, threat intelligence frameworks, blockchain-enabled security, and quantum-resistant cryptography. Expanding beyond conventional attack types to address emerging threats will be key to building adaptive, layered defenses capable of protecting increasingly complex and decentralized grid systems.

In summary, securing the future of smart grids demands a shift from predominantly reactive defense to a proactive, intelligence-driven, and multi-technology strategy. This requires integrating innovative research, cross-sector collaboration, and resilient architectures to anticipate, withstand, and recover from both cyber and physical disruptions. By prioritizing forward-looking approaches, the research community and industry stakeholders can ensure the long-term resilience and trustworthiness of smart grid infrastructure.

FUNDING INFORMATION

The authors declare that no funding was received for this research.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Anass Naqqad	✓	✓	✓		✓	✓	✓	✓	✓		✓			
Abdellah Boulal	✓	✓		✓	✓	✓	✓			✓	✓	✓	✓	
Rachid Habachi	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal Analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject Administration
Fu : **Fu**nding Acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] *World Energy Outlook 2023*. in World Energy Outlook, OECD, 2023. doi: 10.1787/827374a6-en.

[2] M. Shabanzadeh and M. P. Moghaddam, "What is the smart grid? Definitions, perspectives, and ultimate goals," in *28th International Power System Conference*, 2013, pp. 1–5.

[3] G. J. FitzPatrick and D. A. Wollman, "NIST interoperability framework and action plans," in *IEEE PES General Meeting*, PES 2010, 2010 doi: 10.1109/PES.2010.5589699.

[4] R. Habachi, A. Touil, A. Boulal, A. Charkaoui, and A. Echchatbi, "Recommendations and solutions to remove some barriers to the deployment of smart grid in morocco," *International Journal of Power Electronics and Drive Systems*, vol. 10, no. 2, pp. 744–752, 2019, doi: 10.11591/ijpeds.v10.i2.pp744-752.

[5] İ. Avci, "Investigation of cyber-attack methods and measures in smart grids," *Sakarya University Journal of Science*, vol. 25, no. 4, pp. 1049–1060, Aug. 2021, doi: 10.16984/saufenbilder.955914.

[6] T. Berghout, M. Benbouzid, and S. M. Muyeen, "Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects," *International Journal of Critical Infrastructure Protection*, vol. 38, 2022, doi: 10.1016/j.ijcip.2022.100547.

[7] 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, doi: 10.1049/enc2.12091.

[8] V. Sultan, A. Aryal, C. Wu, and H. Lopez, "Smart grid security: A systematic literature review," *Lecture Notes in Networks and Systems*, vol. 700 LNNS, pp. 345–358, 2023, doi: 10.1007/978-3-031-33743-728.

[9] J. Tyav, S. Tufail, S. Roy, I. Parvez, A. Debnath, and A. Sarwat, "A comprehensive review on smart grid data security," in *Conference Proceedings - IEEE SOUTHEASTCON*, 2022, pp. 8–15, doi: 10.1109/SoutheastCon48659.2022.9764139.

[10] B. Kitchenham, *Procedures for Performing Systematic Reviews*, vol. 33, no. 2004. 2014. [Online]. Available: https://www.researchgate.net/publication/228756057.

[11] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering – A systematic literature review," *Information and Software Technology*, vol. 51, no. 1, pp. 7–15, Jan. 2009, doi: 10.1016/j.infsof.2008.09.009.

[12] Y. Zhang, J. Wang, and B. Chen, "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 623–634, 2021, doi: 10.1109/TSG.2020.3010510.

[13] X. Li, C. Jiang, D. Du, W. Li, M. Fei, and L. Wu, "A novel state estimation method for smart grid under consecutive denial of service attacks," *IEEE Systems Journal*, vol. 17, no. 1, pp. 513–524, 2023, doi: 10.1109/JSYST.2022.3171751.

[14] M. K. Hasan, A. K. M. A. Habib, S. Islam, N. Safie, S. N. H. S. Abdullah, and B. Pandey, "DDoS: Distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments," *Energy Reports*, vol. 9, pp. 1318–1326, 2023, doi: 10.1016/j.egyr.2023.05.184.

[15] A. Abdelwahab, W. Lucia, and A. Youssef, "Set-theoretic control for active detection of replay attacks with applications to smart grid," in *CCTA 2020 - 4th IEEE Conference on Control Technology and Applications*, 2020, pp. 1004–1009, doi: 10.1109/CCTA41146.2020.9206373.

[16] J. Tian, B. Wang, J. Li, and Z. Wang, "Adversarial attacks and defense for CNN based power quality recognition in smart grid," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 2, pp. 807–819, 2022, doi: 10.1109/TNSE.2021.3135565.

[17] R. J. R. Kumar and B. Sikdar, "Detection of stealthy cyber-physical line disconnection attacks in smart grid," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4484–4493, 2021, doi: 10.1109/TSG.2021.3082543.

[18] L. Erdodi, P. Kaliyar, S. H. Houmb, A. Akbarzadeh, and A. J. Waltoft-Olsen, "Attacking power grid substations: An experiment demonstrating how to attack the SCADA protocol IEC 60870-5-104," *ACM International Conference Proceeding Series*, 2022, doi: 10.1145/3538969.3544475.

[19] B. E. M. Camachi and D. Popescu, "Cyber security of smart grids infrastructure: Protective measure against attacks," *UPB Scientific Bulletin, Series C: Electrical Engineering and Computer Science*, vol. 82, no. 3, pp. 73–86, 2020.

[20] A. S. Sani, D. Yuan, K. Meng, and Z. Y. Dong, "Idenx: A blockchain-based identity management system for supply chain attacks mitigation in smart grids," in *2020 IEEE Power & Energy Society General Meeting (PESGM)*, IEEE, Aug. 2020, pp. 1–5, doi: 10.1109/PESGM41954.2020.9281929.

[21] X. Di Wang, W. Z. Meng, and Y. N. Liu, "Lightweight privacy-preserving data aggregation protocol against internal attacks in smart grid," *Journal of Information Security and Applications*, vol. 55, 2020, doi: 10.1016/j.jisa.2020.102628.

[22] G. Dileep, "A survey on smart grid technologies and applications," *Renewable Energy*, vol. 146, pp. 2589–2625, 2020, doi: 10.1016/j.renene.2019.08.092.

[23] K. Tazi, F. Abdi, and M. F. Abbou, "Review on cyber-physical security of the smart grid: Attacks and defense mechanisms," in *Proceedings of 2015 IEEE International Renewable and Sustainable Energy Conference*, IRSEC 2015, 2016 doi: 10.1109/IRSEC.2015.7455127.

[24] S. Aziz, M. Irshad, S. A. Haider, J. Wu, D. N. Deng, and S. Ahmad, "Protection of a smart grid with the detection of cyber- malware attacks using efficient and novel machine learning models," *Frontiers in Energy Research*, vol. 10, 2022, doi: 10.3389/fenrg.2022.964305.

[25] S. Banik, T. Banik, S. M. M. Hossain, and S. K. Saha, "Implementing man-in-the-middle attack to investigate network vulnerabilities in smart grid test-bed," in *2023 IEEE World AI IoT Congress (AIIoT)*, IEEE, Jun. 2023, pp. 0345–0351, doi: 10.1109/AIIoT58121.2023.10174478.
[26] A. Xue *et al.*, "Data-driven detection for GPS spoofing attack using phasor measurements in smart grid," *International Journal of Electrical Power & Energy Systems*, vol. 129, p. 106883, Jul. 2021, doi: 10.1016/j.ijepes.2021.106883.
[27] Q. Su, S. Li, Y. Gao, X. Huang, and J. Li, "Observer-based detection and reconstruction of dynamic load altering attack in smart grid," *Journal of the Franklin Institute*, vol. 358, no. 7, pp. 4013–4027, 2021, doi: 10.1016/j.jfranklin.2021.02.008.
[28] H. Shen, Y. Liu, Z. Xia, and M. Zhang, "An efficient aggregation scheme resisting on malicious data mining attacks for smart grid," *Information Sciences*, vol. 526, pp. 289–300, 2020, doi: 10.1016/j.ins.2020.03.107.
[29] K. Kuroptev and F. Steinke, "Coordinated cyber attacks on smart grids considering software supply chains," in *2023 IEEE PES Innovative Smart Grid Technologies Europe (ISGT EUROPE)*, IEEE, Oct. 2023, pp. 1–5, doi: 10.1109/ISGTEUROPE56780.2023.10407630.
[30] Z. Wang, H. He, Z. Wan, and Y. Sun, "Coordinated topology attacks in smart grid using deep reinforcement learning," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 1407–1415, Feb. 2021, doi: 10.1109/TII.2020.2994977.
[31] T. N. Nguyen, B. H. Liu, N. P. Nguyen, B. Dumba, and J. Te Chou, "Smart grid vulnerability and defense analysis under cascading failure attacks," *IEEE Transactions on Power Delivery*, vol. 36, no. 4, pp. 2264–2273, 2021, doi: 10.1109/TPWRD.2021.3061358.
[32] W. Liu, Z. Chen, X. Yu, and X. Zhou, "A cluster-based approach against wormhole attacks in MANETs among smart grid," *Frontiers in Energy Research*, vol. 10, 2022, doi: 10.3389/fenrg.2022.1017932.
[33] M. Hassan *et al.*, "GITM: A GINI index-based trust mechanism to mitigate and isolate sybil attack in RPL-enabled smart grid advanced metering infrastructures," *IEEE Access*, vol. 11, pp. 62697–62720, 2023, doi: 10.1109/ACCESS.2023.3286536.
[34] M. Kumar, S. Prasad, M. R. Ansari, and B. Mohapatra, "Resonance attacks detection and mitigation control scheme on frequency regulation in multi-area smart grid," *International Journal of Control*, vol. 96, no. 9, pp. 2212–2229, 2023, doi: 10.1080/00207179.2022.2087738.
[35] J. Powell, A. McCafferty-Leroux, W. Hilal, and S. A. Gadsden, "Smart grids: A comprehensive survey of challenges, industry applications, and future trends," *Energy Reports*, vol. 11, pp. 5760–5785, 2024, doi: 10.1016/j.egyr.2024.05.051.
[36] Y. Li, X. Wei, Y. Li, Z. Dong, and M. Shahidehpour, "Detection of false data injection attacks in smart grid: A secure federated deep learning approach," *IEEE Transactions on Smart Grid*, vol. 13, no. 6, pp. 4862–4872, Nov. 2022, doi: 10.1109/TSG.2022.3204796.
[37] H. Zhang, B. Liu, and H. Wu, "Smart grid cyber-physical attack and defense: A review," *IEEE Access*, vol. 9, pp. 29641–29659, 2021, doi: 10.1109/ACCESS.2021.3058628.
[38] M. R. Camana Acosta, S. Ahmed, C. E. Garcia, and I. Koo, "Extremely randomized trees-based scheme for stealthy cyber-attack detection in smart grid networks," *IEEE Access*, vol. 8, pp. 19921–19933, 2020, doi: 10.1109/ACCESS.2020.2968934.
[39] E. Drayer and T. Routtenberg, "Detection of false data injection attacks in smart grids based on graph signal processing," *IEEE Systems Journal*, vol. 14, no. 2, pp. 1886–1896, 2020, doi: 10.1109/JSYST.2019.2927469.
[40] M. Ashrafuzzaman, S. Das, Y. Chakhchoukh, S. Shiva, and F. T. Sheldon, "Detecting stealthy false data injection attacks in the smart grid using ensemble-based machine learning," *Computers and Security*, vol. 97, 2020, doi: 10.1016/j.cose.2020.101994.
[41] Z. Wang, W. Cheng, and C. Li, "DoS attack detection model of smart grid based on machine learning method," in *Proceedings of 2020 IEEE International Conference on Power, Intelligent Computing and Systems, ICPICS 2020,* 2020, pp. 735–738, doi: 10.1109/ICPICS50287.2020.9202401.
[42] R. Sriranjani, M. Bharath Kumar, A. K. Paramesh, M. D. Saleem, N. Hemavathi, and A. Parvathy, "Machine learning based intrusion detection scheme to detect replay attacks in smart grid," in *2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science, SCEECS 2023*, 2023, doi: 10.1109/SCEECS57921.2023.10063021.
[43] Q. Jin, M. Li, P. Gao, and Y. Wang, "An anomaly detection framework for internal and external interaction of power grid information network based on the attack-chain knowledge graph," in *Proceedings of the 2022 2nd International Conference on Control and Intelligent Robotics*, New York, NY, USA: ACM, Jun. 2022, pp. 544–550, doi: 10.1145/3548608.3559260.
[44] Y. Liu and L. Cheng, "Relentless false data injection attacks against kalman-filter-based detection in smart grid," *IEEE Transactions on Control of Network Systems*, vol. 9, no. 3, pp. 1238–1250, 2022, doi: 10.1109/TCNS.2022.3141026.
[45] M. Dehghani, T. Niknam, M. Ghiasi, P. Siano, H. H. Alhelou, and A. Al-Hinai, "Fourier singular values-based false data injection attack detection in AC smart-grids," *Applied Sciences (Switzerland)*, vol. 11, no. 12, 2021, doi: 10.3390/app11125706.
[46] C. Pei, Y. Xiao, W. Liang, and X. Han, "PMU placement protection against coordinated false data injection attacks in smart grid," *IEEE Transactions on Industry Applications*, vol. 56, no. 4, pp. 4381–4393, 2020, doi: 10.1109/TIA.2020.2979793.
[47] K. Hafeez, D. O'Shea, T. Newe, and M. H. Rehmani, "E-DPNCT: an enhanced attack resilient differential privacy model for smart grids using split noise cancellation," *Scientific Reports*, vol. 13, no. 1, 2023, doi: 10.1038/s41598-023-45725-9.
[48] E. Rios, A. Rego, E. Iturbe, M. Higuero, and X. Larrucea, "Continuous quantitative risk management in smart grids using attack defense trees," *Sensors (Switzerland)*, vol. 20, no. 16, pp. 1–25, 2020, doi: 10.3390/s20164404.
[49] A. Almajali, Y. Wadhawan, M. S. Saadeh, L. Shalalfeh, and C. Neuman, "Risk assessment of smart grids under cyber-physical attacks using Bayesian networks," *International Journal of Electronic Security and Digital Forensics*, vol. 12, no. 4, p. 357, 2020, doi: 10.1504/IJESDF.2020.110660.
[50] X. G. Shan and J. Zhuang, "A game-theoretic approach to modeling attacks and defenses of smart grids at three levels," *Reliability Engineering and System Safety*, vol. 195, 2020, doi: 10.1016/j.ress.2019.106683.
[51] M. Pilz *et al*., "Security attacks on smart grid scheduling and their defences: a game-theoretic approach," *International Journal of Information Security*, vol. 19, no. 4, pp. 427–443, Aug. 2020, doi: 10.1007/s10207-019-00460-z.
[52] Y. Li, X. Wang, and J. Zeng, "Improved Wasserstein generative adversarial networks defense method against data integrity attack on smart grid," *Recent Advances in Electrical & Electronic Engineering (Formerly Recent Patents on Electrical & Electronic Engineering)*, vol. 15, no. 3, pp. 243–254, May 2022, doi: 10.2174/2352096515666220506213526.
[53] V. P. K. Madhavarapu, S. Bhattacharjee, and S. K. Dasy, "A generative model for evasion attacks in smart grid," in *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, IEEE, May 2022, pp. 1–6, doi: 10.1109/INFOCOMWKSHPS54753.2022.9798325.

[54] A. Agrawal and S. Affijulla, "A concept for discrimination of electrical fault from cyber attack in smart electric grid," *Journal of Electrical Engineering*, vol. 73, no. 4, pp. 299–304, Aug. 2022, doi: 10.2478/jee-2022-0039.
[55] I. Mustafa, A. Adeel, and K. Zineddine, "Security of smart-meters against side-channel-attacks (SCA)," *International Journal of Informatics and Applied Mathematics*, vol. 2, no. 1, pp. 27–36, 2019.
[56] J. C. Balda, A. Mantooth, R. Blum, and P. Tenti, "Cybersecurity and power electronics: Addressing the security vulnerabilities of the internet of things," *IEEE Power Electronics Magazine*, vol. 4, no. 4, pp. 37–43, 2017, doi: 10.1109/MPEL.2017.2761422.
[57] A. Zahoor *et al.*, "An access control scheme in IoT-enabled smart-grid systems using blockchain and PUF," *Internet of Things (Netherlands)*, vol. 22, 2023, doi: 10.1016/j.iot.2023.100708.
[58] H. M. S. Badar, S. Qadri, S. Shamshad, M. F. Ayub, K. Mahmood, and N. Kumar, "An identity-based authentication protocol for smart grid environment using physical uncloneable function," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4426–4434, 2021, doi: 10.1109/TSG.2021.3072244.
[59] M. B. Mollah *et al.*, "Blockchain for future smart grid: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 18–43, Jan. 2021, doi: 10.1109/JIOT.2020.2993601.
[60] X. Zhang, Z. Y. Dong, Z. Wang, C. Xiao, and F. Luo, "Quantum cryptography based cyber-physical security technology for smart grids," *IET Seminar Digest*, vol. 2015, no. 8, 2015, doi: 10.1049/ic.2015.0263.
[61] B. Achaal, M. Adda, M. Berger, H. Ibrahim, and A. Awde, "Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges," *Cybersecurity*, vol. 7, no. 1, p. 10, May 2024, doi: 10.1186/s42400-023-00200-w.
[62] V. Lamba, N. Šimková, and B. Rossi, "Recommendations for smart grid security risk management," *Cyber-Physical Systems*, vol. 5, no. 2, pp. 92–118, Apr. 2019, doi: 10.1080/23335777.2019.1600035.

BIOGRAPHIES OF AUTHORS

Anass Naqqad born in Settat, Morocco, in 1997, is currently a Ph.D. student at the Faculty of Engineering and Sciences, Hassan 1st University, Settat, and a cyber security consultant at a leading consultancy group specializing in identity and access management. He received his engineering degree in cyber security from CentraleSupélec. His research interests focus on cyber security and smart grids. He can be contacted at email: a.naqqad.doc@uhp.ac.ma.

Abdellah Boulal born in Settat, Morocco, in 1971, is currently a professor at the Laboratory of Engineering, Industrial Management, and Innovation (IMII) within the Faculty of Sciences and Technology at Hassan 1st University, Settat. He earned his master's degree in energies from Hassan 1st University and went on to receive his Ph.D. in sciences and technology from the same institution in 2017. He is deeply involved in research and teaching, with a focus on industrial innovation and energy management, contributing to numerous projects within the IMII laboratory. He can be contacted at email: abdellah.boulal@uhp.ac.ma.

Rachid Habachi born in Berrechid, Morocco, in 1986, is currently a professor of electrical engineering at the Faculty of Sciences and Technology, Hassan 1st University, Settat. He earned his master's degree in automatic, signal Processing, and industrial computing from Hassan 1st University in 2011, and later received his Ph.D. in electrical engineering from the same institution in 2020. He is also a member of the Laboratory of Engineering, Industrial Management, and Innovation (IMII). His research interests focus on applications of embedded systems, artificial intelligence, and intelligent control. He can be contacted at email: rachid.habachi@uhp.ac.ma.