Future Energy
Open Access Journal
ISSN 2832-0328

November 2026| Volume 05 | Issue 04 | Pages 18-25

Journal homepage: https://fupubco.com/fuen

https://doi.org/10.55670/fpll.fuen.5.4.3

Future Publishing LLC

Review

Current perspectives on smart grid cybersecurity and critical infrastructure protection

Puneet Garg*

Department of CSE-AI, KIET Group of Institutions, Delhi NCR, Ghaziabad, India

ARTICLE INFO

Article history:
Received 18 May 2026
Received in revised form
29 August 2026
Accepted 18 September 2026

Keywords:
Smart Grid cybersecurity, Cyber-attacks,
Critical infrastructure protection,
Intrusion detection, Cyber resilience

*Corresponding author
Email address:
puneet.garg@kiet.edu

DOI: 10.55670/fpll.fuen.5.4.3

ABSTRACT

The increasing convergence of renewable energy sources, information and communication technology, Internet of Things devices, smart meters, and phasor measurement units has enhanced the efficiency, reliability, and real-time operation of Smart Grids. However, this interconnected cyber-physical infrastructure has also increased cybersecurity vulnerabilities and attack surfaces. This paper reviews AI/ML-based security approaches for Smart Grid cybersecurity and critical infrastructure protection, focusing on major threats such as False Data Injection Attacks, Denial-of-Service attacks, Man-in-the-Middle attacks, spoofing, malware, and malicious command injection. The study examines existing protection mechanisms, including authentication and access control, intrusion detection, attack mitigation, secure communication, data protection, and privacy preservation. The study further discusses cyber-physical system protection, resilience, incident response, continuous monitoring, network segmentation, and AI/ML-based security approaches. A review of recent research highlights advances in anomaly detection, trust management, multilayer security, and intelligent threat detection. However, challenges remain in scalability, real-time processing, interoperability, adaptive defense, limited datasets, and real-world validation. The findings emphasize the need for integrated, intelligent, scalable, and adaptive cybersecurity approaches to strengthen Smart Grid resilience, reliability, availability, and operational continuity.

1. Introduction

Eco-Modern critical infrastructures increasingly rely on interconnected digital, communication, and control technologies to improve efficiency, reliability, and real-time operation. As these systems become more connected and data-driven, cybersecurity is essential for protecting infrastructure, services, information, and operational continuity [1]. Smart-grid security refers to protecting power infrastructure, communication networks, control systems, devices, and data from cyber and physical threats [2]. As smart grids integrate digital technologies with physical power-system components, a cyber breach can directly affect physical operations. Therefore, smart-grid security aims to ensure confidentiality, integrity, availability, reliability, resiliency, privacy, and safety while maintaining stable power-system operation. Rising energy demand and the development of Smart grids have driven the integration of cutting-edge communication and information technologies. These systems use digital technologies to monitor, control, and optimize electricity distribution and consumption in real time, thereby improving operational efficiency, grid reliability, and demand response management. However, the transition from conventional grids introduces cybersecurity challenges. Smart grids provide numerous benefits, including the efficient integration of Renewable Energy Sources (RESs). Integrating photovoltaic (PV), wind, battery energy storage systems (BESS), distributed energy resources (DERs), and microgrids introduces new cybersecurity concerns. A cyberattack targeting renewable-generation measurements or forecasts can lead to inaccurate forecasts and affect dispatch decisions. Inverter control attacks can affect active and reactive power generation and voltage control, and communication-system control attacks on DERs can undermine the coordinated operation of distributed resources and microgrids. These consequences might affect grid stability, power balance, and the capacity to incorporate renewable energy. However, their dependence on advanced communication infrastructure and extensive data exchange increases vulnerability to cyberattacks. The integration of the Internet of Things (IoT), smart meters, and Phasor Measurement Units (PMUs) further expands the attack surface, making cyberattack detection and identification difficult within narrow time windows [3]. In addition, the

volatility, intermittency, and unpredictability of RES behavior create uncertainty in energy management and grid operation.

Among the threats targeting smart grids, Denial-of-Service (DoS) and False Data Injection (FDI) attacks are particularly significant. DoS attacks aim to disrupt data transfer, whereas FDI attacks manipulate measurements or measurement-related data used by grid monitoring and state-estimation processes. Such attacks can target command and feedback signals, protective relays, and sensor or actuator software calibrations. FDI attacks can degrade system performance and, under severe conditions, contribute to instability and service disruption [4]. The interconnected nature of smart-grid systems exposes them to data breaches, malware, and Advanced Persistent Threats (APTs), which traditional cybersecurity approaches may struggle to detect. As critical infrastructure, the smart grid can fail, causing widespread power outages, financial losses, and national security risks [5]. Thus, effective cybersecurity measures are essential for safe and reliable operation. Intelligent optimization techniques, including genetic algorithms, neural networks, game theory, reinforcement learning, and support vector machines, have contributed to security analysis and rapid identification of critical infrastructure elements. The remainder of this paper is organized as follows: Section 2 discusses the Smart Grid cybersecurity landscape. Section 3 presents security and protection mechanisms. Section 4 covers critical infrastructure protection and resilience. Section 5 reviews recent research and research gaps. Section 6 concludes the paper and presents future work.

2. Smart Grid cybersecurity

The evolution of Smart Grid cybersecurity highlights the critical role of two-way communication networks and computer-based automation in improving grid efficiency while also increasing vulnerability to cyber threats. This work identifies the latest obstacles to improving smart grid cybersecurity, emphasizing quantifiable factors that influence the adoption of cybersecurity techniques. Evaluates the effectiveness of recently proposed cybersecurity methods in detecting and identifying False Data Injection (FDI) attacks, considering their accuracy, computational time, and robustness. The complexity of improving power systems' cyber resilience and the need to customize cybersecurity solutions to each system's particular requirements [6]. Recent studies on Smart Grid cybersecurity focus on widely studied attacks, including false data injection (FDIA), DoS, DDoS, and spoofing attacks, including false data injection (FDIA), DoS, DDoS, and spoofing attacks. It provides an extensive survey of defense mechanisms that can be used to detect and mitigate these cyberattacks. It highlights the critical need to secure cyber-physical smart grid systems against growing security threats and attacks, emphasizing the role of Internet of Things (IoT) technologies in both enhancing grid functionality and introducing new vulnerabilities.

2.1 Smart grid architecture and communication infrastructure

The semantic approach to smart grids, guided by standardization organizations and object-mapping processes, uses a holistic architectural model that classifies energy networks into seven sub-sectors. These sectors include distribution, transmission, operations, service providers, consumers, markets, and generation (both bulk and non-bulk). This conceptual approach provides the architectural foundation for developing new standards and for characterizing and evaluating the compatibility of existing ones. Using a variety of communication architectures, such as wired, wireless, and power line communication infrastructure networks, the corresponding interfaces, and the relevant protocols, the various domains within this architecture communicate with one another through electrical or communication flows [7]. Figure 1 shows the smart grid architecture, illustrating how generation, transmission, distribution, markets, operations, service providers, and customers connect through support systems.

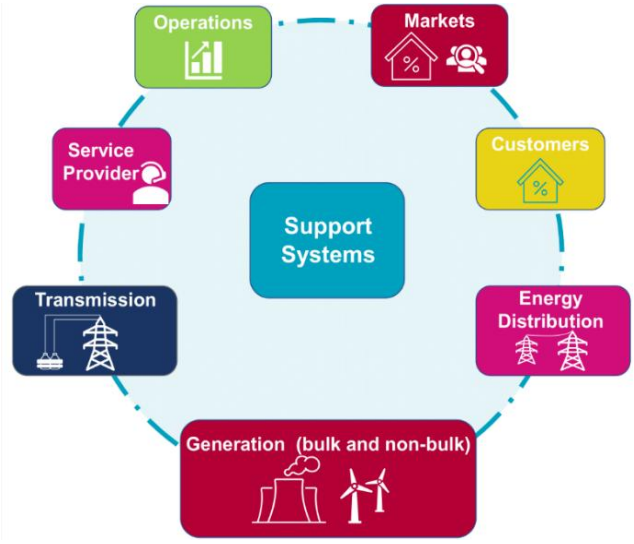

Figure 1. Smart Grid architecture domains

Generation: Produces electricity from conventional and renewable sources.
Transmission: Transfers electricity over high-voltage networks.
Energy distribution: Delivers electricity to end users.
Customers: Consume electricity and participate through smart-grid technologies.
Markets: Support electricity trading, pricing, and demand response.
Operations: Monitor, control, and optimize grid activities.
Service providers: Provide energy, communication, and related services.
The five fundamental guidelines for developing a technically sound, integrated communication system for use in smart grid networks are:
Interoperability: The ability of smart grid hardware and software components to communicate directly with one another is called interoperability. This makes information sharing simple and effective without upsetting the end user.
Interconnectivity: The ability of all energy ecosystem players (stations, substations, machines, devices, sensors, applications, and people) to interact with each other.
Classified access to information: The availability of quick and simple access to helpful information at every stage of the energy process.

System monitoring: The cyber-physical technologies that facilitate every operation, gathering and displaying data virtually instantly.

Decentralized decision-making: Cyber-physical systems typically make the best choices on their own. Generally, higher levels in the hierarchy step in only when objectives conflict [8].

2.2 Cybersecurity threats and attack vectors

Complex networks and contemporary technology have increased the power infrastructure's susceptibility to cyberattacks (CAs). To safeguard the grid, it is essential to understand the types of cyberattacks that may be carried out against it and their access points. Protections from certain dangers. Man-in-the-middle (MiTM) attacks, malicious command injection, malware, DoS, TSA, RA, TDA, FDIA, and LRA. Each category has unique characteristics and potential impacts. The impacts are analyzed. The second section, however, categorizes attacks by target. Cybercriminals may target SG components with specific vulnerabilities. Every component- including consumers, power markets and service providers, SCADA systems, WAN communication technologies, measuring equipment, and AGC systems- is covered in terms of potential cyberattacks.

Man-in-the-middle attack (MiTM): An SG faces several risks from MiTM attacks. The potential security risks posed by a MiTM attack on a power system focus on the flaws in the Modbus TCP/IP protocol used for communications. In a MiTM attack, an attacker inserts himself into a dialogue between two devices to eavesdrop or spoof one of the devices, making the information flow appear normal [9].

False data injection attack (FDIA): State estimation estimates the state of the power system, in this case voltages and phase angles of the buses, from measurements obtained by the meters. FDI attacks can falsify measurements used in state estimation and, consequently, produce incorrect estimates of bus voltage, phase angle, and power flow. These errors could lead to incorrect voltage-control and generation-dispatch decisions, affecting grid reliability.

Denial of service attack (DoS): SGs include a variety of measuring equipment, such as SMs, smart appliances, data aggregators, PMUs, RTUs, IEDs, and PLCs. Several DoS-targeting vulnerabilities exist in these devices. A denial-of-service (DoS) attack in a power system prevents control orders from reaching actuators or makes measurement device data unavailable to the intended user, ultimately leading to system instability.

The impact of these cyberattacks on the physical world can be directly connected to Smart Grid operations. FDI attacks can lead to the falsification of measurements used in state estimation, and consequently to incorrect estimates of bus voltage, phase angle, and power flow. These incorrect numbers could lead to incorrect voltage control and generation dispatch decisions, thereby affecting grid reliability. Denial-of-Service (DoS) attacks can make measurement data unavailable or make it difficult to send control commands to actuators, affecting real-time monitoring, protection coordination, load management, and frequency and voltage regulation. An attack can alter measurement or control messages exchanged between devices on the grid, leading to incorrect switching, protection tripping, or power-flow decisions. Falsified identities or measurements can be sent to grid devices and operators, affecting monitoring, state estimation, and operational decisions. Deliberate command injection may introduce unauthorized commands into control systems, causing improper switching and disturbances in generator/load control, voltage, frequency, and power flow. This means that cyber threats to Smart Grids can extend beyond communication and data security to affect physical system stability, protection, reliability, and operational continuity.

2.3 Vulnerabilities and security challenges

The major vulnerabilities and security challenges in Smart Grids are:

Physical security risks: Field devices located outside utility premises are vulnerable to physical tampering and unauthorized access.

IoT device management: The large number of interconnected IoT devices makes monitoring, management, and security enforcement difficult.

Data privacy: Smart meters collect detailed consumer information, creating privacy and data-security concerns.

Legacy technology: The coexistence of legacy power-system technologies with modern IT systems can create compatibility and security gaps.

Organizational and coordination challenges: Inadequate coordination and communication among teams can lead to security weaknesses and critical decision-making errors.

IP-based attacks: IP-enabled devices are vulnerable to attacks such as IP spoofing and Denial-of-Service (DoS).

Large attack surface: Integrating communication networks, smart meters, sensors, and control systems increases opportunities for cyber intrusion [10].

3. Smart Grid security and protection mechanisms

Smart grid security and protection mechanisms are essential for maintaining confidentiality, integrity, availability, and reliability of cyber-physical power systems. Because smart grids integrate communication networks, smart meters, sensors, intelligent electronic devices, and distributed energy resources, security mechanisms must protect both cyber and physical components.

Authentication and access control: Access control and authentication mechanisms safeguard privacy so that remote users can operate in a home network-based smart grid environment and securely access HAN [11]. The NIST privacy subgroup of the CSWG (cybersecurity working group) splits privacy into four key categories: privacy of personal communications, privacy of personal information, privacy of person, and privacy of behavior.

Data encryption: Sensitive data should always be encrypted during transport and storage. When implementing such mechanisms, proprietary protocols should be avoided. Ensure that Secure Sockets Layer (SSL)/Transport Layer Security (TLS) implementations are properly configured and up to date.

Intrusion detection and prevention: Systems like Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) help locate and stop system and component attacks [12]. Thus, evaluating a system's logging and monitoring mechanisms is an important security criterion for SGSC.

3.1 Authentication and access control

For end-to-end communication, Identity-Based Encryption (IBE) with zero-configuration encryption and authentication has been proposed [13]. Researchers have proposed encrypting node-to-node links using a secret key. However, in large networks, packet overhead may increase for both IBE and node-to-node authentication. In the Diffie-Hellman key protocol, message authentication is proposed in addition to hash-based message authentication. This approach provides greater scalability, lower memory use, and shorter decryption delays. Four broad countermeasures to thwart attacks on smart meters have been proposed in:

- Authentication and strong encryption of communication that deals with HAN and NAN and buses within smart meters,
- Secure key management, which forms the critical backbone of a secure AMI,
- Securing the firmware to avoid being manipulated by attackers or mistakenly by authorized personnel, and
- Security-driven firmware development cycle that conducts frequent walkthroughs and security assessments [14].

Access control is a fundamental security mechanism in Smart Grid systems that ensures only legitimate and authorized users, devices, and entities can access grid resources and perform permitted operations [15].

Access control mechanisms: Authentication, authorization, and control policies collectively form an access control mechanism. These mechanisms are essential in Smart Grids because numerous users and devices with different roles and privileges interact with a large number of interconnected grid devices.

Centralized and decentralized access control: Access control mechanisms can be centralized or decentralized and may use static or dynamic attributes and policies.

Centralized access control: In a centralized approach, access-control data and policies are stored and managed at a central location through components such as control panels and reader control modules. This approach is relatively simple and easier to manage.

3.2 Intrusion detection and attack mitigation

Intrusion detection in smart grids primarily uses signature-based and anomaly-based approaches. Signature-based IDS effectively identifies known attacks but has limited capability against zero-day and novel threats [16]. To improve detection performance [17], it combines Isolation Forest (IF) for outlier removal, Pearson's Correlation Coefficient (PCC) for feature selection, and RF classification. Evaluation on the imbalanced Bot-IoT dataset using MCC demonstrated improved IDS performance compared with other models. For attack mitigation, microgrid-based strategies have also been investigated to enhance grid reliability, resilience, and protection against consequential failures [18].

3.3 Data protection and privacy

The General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) both exist to protect user information and require organizations to take responsibility for personal data management. All organizations need to follow strict rules for data collection and processing when sharing data, as these requirements enforce privacy-conscious cybersecurity practices. The CCPA gives consumers rights such as access, deletion, correction, and opting out of certain sales or sharing of personal information, subject to applicable conditions and exceptions [19]. Although data protection regulations exist, privacy threats persist due to evolving cyber vulnerabilities, internal attacks, and weak security systems. Organizations face a primary challenge in achieving effective cybersecurity while safeguarding user privacy at an optimal level globally.

- GDPR and CCPA are decent provisions for safeguarding personal information and managing information responsibly.
- Data minimization, consent, and the right to erasure are important GDPR concepts, but consent is not universally required for all data processing.
- CCPA gives consumers rights such as access, deletion, correction, and opting out of the sale/sharing of personal information, subject to applicable conditions and exceptions.
- Data encryption, access control, anonymization, secure data sharing, and privacy-preserving technologies can enhance privacy protection.
- In Smart Grid environments, privacy concerns are particularly relevant because smart meters can reveal detailed customer energy-consumption patterns and personally identifiable information (PII).

4. Critical infrastructure protection in smart grids

Safeguarding smart-grid assets, communication networks, control systems, and operational technologies against cyber and physical threats is essential. CIP practices for utilities generally emphasize cybersecurity governance, physical protection, personnel awareness, incident response, system monitoring, and recovery. In addition, advanced technologies such as Artificial Intelligence (AI) and Machine Learning (ML) are increasingly being explored to improve threat detection, anomaly identification, and proactive defense in smart-grid environments. Key aspects of Critical Infrastructure Protection include:

Cybersecurity standards and regulations: Utilities should implement established cybersecurity standards, policies, and controls to protect critical grid infrastructure.

Physical security: Substations, smart meters, communication equipment, control centers, and other field devices should be protected against unauthorized physical access, tampering, and damage.

Incident response and recovery: Effective incident-response plans are required to detect, contain, investigate, and recover from cyber incidents while minimizing disruption to grid operations.

Security monitoring: Continuous monitoring of network traffic, devices, and system activities can help identify abnormal behavior and potential attacks at an early stage.

AI- and ML-based protection: AI and ML techniques can analyze large volumes of smart-grid data in real time to detect anomalies, identify emerging threats, and support automated security responses.

Privacy protection: Techniques such as pseudonymization and data minimization can reduce privacy risks when sensitive smart-meter and operational data are analyzed.

Adaptive defense: Future smart-grid protection can combine AI/ML-based detection with adaptive security mechanisms capable of responding to changing attack patterns.

Emerging cryptographic technologies: Advanced cryptographic approaches, including post-quantum cryptography and quantum key distribution, are being investigated to strengthen the long-term security of critical energy infrastructure [20].

4.1 Cyber-physical system protection

Requirements for the cyber-physical security of the SG have been evolving to address the challenges posed by the SG's new operational structure, which integrates cyber and physical components [21]. Security demands in traditional power grids were presented as follows: human safety, equipment and power line protection, and system protection. The various security requirements that arose to meet the new threats were:

Real-time (RT) availability: The ability of data or services to be accessed when needed by authorized parties without interruption or unexpected downtime is called availability. Unlike IT systems, the dynamics of the physical system in the SG are closely tied to RT availability.

Integrity: Prevents unauthorized alteration or modification of data and ensures the information is consistent, reliable, and correct. Integrity in SCADA systems consists of the trustworthiness of syntactically and semantically created, transmitted, stored, and displayed data, as well as the legitimacy of the sender and receiver.

Confidentiality: Encompasses all aspects related to disclosing data to unauthorized parties. Integrity and availability are more important than confidentiality for SG.

Reliability: Redundancy generally improves reliability, which is the ability of a system to run without downtime for a given period under specific conditions.

Resiliency: The ability of the SG to withstand disturbances and bounce back from them to provide an acceptable level of service. The SG's resiliency enhances its reliability.

Scalability: Scalability is a key component of modern critical infrastructure and is included here. The SG has many devices, and modeling the resiliency architecture is difficult.

Privacy: Privacy issues pertain to data transmitted across the SG's various utilities. Concerns may arise from AMIs that include consumer information.

Safety: All policies and protections used in the SG to ensure that humans or facilities of the plant are not harmed and do not suffer loss due to harms and hazards in these policies.

4.2 Resilience and Incident Response

Cybersecurity is a primary component of overall resilience. The typical resilience curve of a power system is "the ability of a system to withstand, absorb, and quickly bounce back from an external, high-impact, low-frequency event of potentially devastating nature, such as an extreme weather event or a cyber-attack". This curve represents the system's behavior over time in a scenario that causes deterioration. This provides an overview of the various resilience states and their primary defense mechanisms, including robustness, resistance, resourcefulness, redundancy, and adaptive self-organization. Resilience can be evaluated using quantitative metrics such as system reliability, power quality, number of affected customers, outage duration, and recovery time [22]. From a resilience standpoint, the evidence is limited that better monitoring, segmentation, and incident response (IR) practices can prevent physical outages caused by cyber threats, even against highly targeted OT malware. This case reinforces the paper's main argument that cyber resilience goes beyond preventing intrusion; it also addresses the consequences through detection and response capabilities that can be adapted to the operational environment [23]. Table 1 summarizes the main dimensions of Smart Grid cyber resilience and their contribution to detection, resistance, response, recovery from cyber-attacks, and reliable grid operation.

5. Literature review

This literature review focuses on artificial intelligence, anomaly detection, secure communications, trust management, and multilayer security to enhance cybersecurity, resilience, and real-time threat detection in the Smart Grid. J. Li [24] presents a method for creating synthetic attack data using a GAN approach that is derived from robustness, redundancy, and resourcefulness.

Table 1. Key dimensions of smart grid cyber resilience

Aspect	Description	Role in Smart Grid Cybersecurity
Cyber Resilience	Ability to withstand, adapt to, and recover from cyber-attacks.	Maintains critical grid operations.
Robustness & Resistance	Ability to tolerate disturbances and limit performance loss.	Reduces attack impact.
Resourcefulness	Effective use of technical, human, and operational resources.	Supports rapid recovery.
Redundancy	Use of backup systems and alternative communication paths.	Maintains grid continuity.
Adaptive Self-Organization	Ability to adapt operations and defenses to changing threats.	Improves resilience against evolving attacks.
Monitoring & Detection	Continuous monitoring of grid and OT activities.	Enables early attack detection.
Network Segmentation	Isolation of critical systems and network zones.	Limits attack propagation.
Incident Response	Detection, containment, mitigation, and recovery from incidents.	Minimizes damage and recovery time.
Resilience Metrics	Measures such as reliability, availability, outage duration, and recovery time.	Evaluates resilience performance.
Cyber-Physical Impact Mitigation	Measures to limit the physical effects of cyber-attacks.	Protects grid reliability and availability.

The experimental evaluation on the IEEE-14 bus system (75 IEDs) shows a 25.0% increase in system resilience, 18.5% increase in F1 score for imbalanced attack classes, and 40.3% reduction in recovery time; the overall accuracy is improved from 82.4% to 91.7%, and the APT detection rate is enhanced from 31% to 74%.

K. Sultan et al. [25] proposed a novel formal trust-based model for assessing the security of Smart Grids under uncertainty. Extend the Probabilistic Computation Tree Logic of Trust (PCTLT) with a group operator to form the Probabilistic Computation Tree Logic of Group Trust (PCTLT+). Use this reasoning to precisely describe trust-related security properties and verify them using model checking. A Smart Grid Energy Management System scenario is presented to highlight major security issues: device authenticity, data integrity, privacy protection, and command legitimacy.

S. Horbachenko et al. [26] proposed an integrated framework for strengthening Smart Grid cybersecurity through the combination of anomaly detection, standards compliance, and economic-mathematical modeling. Using the SustDataED2 dataset with anomaly injection scenarios, the Isolation Forest algorithm was applied to detect rare patterns of cyber intrusions in high-dimensional data streams. To ensure realistic calibration, empirical attack distributions were derived from recent industry reports, including Cisco Talos, Fortinet, IBM X-Force, and the Verizon Data Breach Investigations Report.

O. V. G. Swathika et al. [27] discuss how Smart Grid (SG) is the solution for such requirements in the energy sector. SG consists of three main components: Information Technology (IT), Operational Technology (OT), and Advanced Metering Infrastructure (AMI). Synchronizing these three components is essential to deliver electricity seamlessly to consumers connected to the electric network. Cyberattacks are increasing sharply across SG infrastructure, triggering disruptions or malicious manipulation of the entire electricity network. Maintaining reliable data traffic, power transmission, and distribution is crucial.

S. Simon Thomas et al. [28] survey existing cybersecurity measures and strategies employed in smart grids, secure communication technologies, various cyberattacks in smart grids, and the influence of cyberattacks on the physical and cyber components of the smart grid. The review also discusses and explores emerging techniques to detect cyber-physical attacks as potential findings to strengthen the cybersecurity resilience of smart grids.

A. Sharma and Babbar [29] noted that new technologies and methods for cybersecurity will enable a more effective approach to dealing with IoT security. With the introduction of modern technology, many devices can now connect to the internet; for example, smart schooling, smart transportation, smart cities, and smartphones. Smart transportation is often seen as the largest application space for ML solutions to address many attacks and spark thought-provoking discussions.

Table 2. Summary of recent research on smart grid cybersecurity

Author	AI/ML Approach	Focus Area	Challenges	Key Findings	Limitations	Future Direction
Li (2026) [24]	GAN-based	Resilience and attack-data generation	Imbalanced attacks and recovery time	Improved resilience, detection, accuracy, and recovery performance	Evaluated mainly on IEEE-14 bus system	Validate on larger and diverse smart-grid environments
Sultan (2025) [25]	Formal trust/model checking	Formal trust-based security verification	Uncertainty, trust, and security-property verification	PCTLT+ enables formal specification and model checking of trust properties	Limited practical and large-scale validation	Integrate formal trust models with real-time security systems
Horbachenko (2025) [26]	Unsupervised anomaly detection	Anomaly detection and cybersecurity risk modelling	Rare attacks and high-dimensional data	Isolation Forest effectively identifies abnormal patterns	Dependent on injected anomaly scenarios and external attack distributions	Test with real-world attack data and adaptive detection methods
Swathika et al. (2024) [27]	ML and Deep Learning (DL)	Smart-grid architecture and cyberattack risks	IT, OT, and AMI integration	Highlights the need for reliable and secure grid operations	Limited emphasis on specific detection and mitigation techniques	Develop integrated real-time security mechanisms
Simon Thomas (2024) [28]	Review of emerging detection methods	Smart-grid cybersecurity review	Diverse cyberattacks and cyber-physical impacts	Identifies emerging approaches for improving cybersecurity resilience	Mainly review-based with limited experimental validation	Conduct practical evaluation of advanced detection techniques
Sharma (2023) [29]	ML-based	ML-based attack detection	Diverse IoT attack categories	ML techniques support attack classification and detection	Focuses on BoT-IoT rather than smart-grid-specific data	Develop smart-grid-specific and adaptive ML models
Manbachi (2022) [30]	AI-based	Virtualized smart-grid security and communication	Secure remote access and reliable communication	Demonstrates secure virtualization and communication approaches	Focused on a specific virtualization/learning environment	Extend secure virtualization to real-world smart-grid applications

For this purpose, the study uses an efficient BoT-IoT dataset, along with a collection of attack categories and subcategories, to train and test the system's dependability.

M. Manbachi and Hammami [30] introduced VELP, its features and functionalities, and explained how monitoring and control layers can be migrated into cyberspace. Moreover, this paper proposes a reliable communication network and a cybersecure topology that can be utilized in similar virtualization platforms. This paper shows that these technologies can be applied to other digital experiential learning programs where reliable, secure remote access to tangible resources is necessary to enable relevant experiential learning approaches.

AI/ML approaches provide different capabilities for Smart Grid cybersecurity. Supervised learning requires labeled attack data and works well for known attack detection, while unsupervised anomaly detection can detect unknown patterns with comparatively little labeled data, though it may be prone to false alarms. Deep learning can learn complex attack patterns and typically requires more data and resources. While GANs can produce synthetic attack data and improve detection of imbalanced and evolving attacks, training complexity may hinder their use in real-time applications. Therefore, available data, detection requirements, and computing requirements all factor into approach selection. Table 2 summarizes recent Smart Grid cybersecurity studies, their key findings, challenges, and limitations, highlighting the need for scalable and practical security solutions.

6. Conclusion

Smart Grid cybersecurity is essential for protecting modern power systems that integrate communication networks, smart meters, IoT devices, renewable energy sources, PMUs, and cyber-physical control systems. This review examined major cybersecurity threats, including False Data Injection Attacks, Denial-of-Service attacks, Man-in-the-Middle attacks, spoofing, malware, and malicious command injection, along with their potential effects on grid reliability and operational continuity. Existing protection mechanisms such as authentication and access control, secure communication, intrusion detection, attack mitigation, data protection, privacy preservation, continuous monitoring, and network segmentation were discussed. The review also emphasized cyber-physical system protection, resilience, and incident response as important components of critical infrastructure protection. Recent research shows the growing potential of AI/ML-based anomaly detection, trust management, multilayer security, and intelligent attack detection to improve Smart Grid security. However, important challenges remain, including scalability, real-time processing, heterogeneous infrastructures, interoperability, limited datasets, adaptive defense, and insufficient real-world validation. Addressing these challenges requires integrated security approaches that can coordinate detection, prevention, response, and recovery while maintaining reliability, availability, resilience, and safety of Smart Grid operations. Future research should develop scalable, adaptive AI/ML-based security frameworks; large real-world datasets; automated incident response; privacy-preserving techniques; standardized evaluation benchmarks; and interoperable protection mechanisms across IT, OT, AMI, and emerging Smart Grid infrastructures.

Ethical issue

The author is aware of and complies with best practices in publication ethics, specifically regarding authorship (avoidance of guest authorship), dual submission, manipulation of figures, competing interests, and compliance with research ethics policies. The author adheres to publication requirements that the submitted work is original and has not been published elsewhere in any language.

Data availability statement

The manuscript contains all the data. However, more data will be available upon request from the corresponding author.

Conflict of interest

The author declares no potential conflict of interest.

References

[1] A. Joon, “Smart Predictive Maintenance: AI-Driven Adaptation for Industrial Equipment,” in 2025 IEEE North-East India International Energy Conversion Conference and Exhibition (NE-IECCE), IEEE, Jul. 2025, pp. 1–6. doi: 10.1109/NE-IECCE64154.2025.11183108.

[2] 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, 2024, doi: 10.1186/s42400-023-00200-w.

[3] N. Karra and N. Karra, “Priority-Aware Heuristic Load Balancing Framework for IoT Applications in Fog–Cloud Environments,” in 2025 International Conference on Intelligent & Innovative Practices in Engineering & Management (IIPEM), Singapore, Singapore: IEEE, 2025, pp. 1–6, November. doi: 10.1109/IIPEM65914.2025.11548242.

[4] F. Mohammadi, “Emerging Challenges in Smart Grid Cybersecurity Enhancement: A Review,” Energies, vol. 14, no. 5, 2021, doi: 10.3390/en14051380.

[5] A. Chehri, I. Fofana, and X. Yang, “Security Risk Modeling in Smart Grid Critical Infrastructures in the Era of Big Data and Artificial Intelligence,” Sustainability, vol. 13, no. 6, 2021, doi: 10.3390/su13063196.

[6] H. Nwapali, N. Naiho, O. Layode, and G. S. Adeleke, “Addressing cybersecurity challenges in smart grid technologies : Implications for sustainable energy infrastructure,” P-ISSN: 2708-8944, E-ISSN: 2708-8952, vol. 5, no. 6, pp. 1995–2015, 2024, doi: 10.51594/estj/v5i6.1218.

[7] R. K. Kanneganti, “Impact of Custom Interface Widgets on User Efficiency in Content Navigation Platforms,” Eastasouth J. Inf. Syst. Comput. Sci., vol. 1, no. 01, pp. 179–186, Aug, 2023, doi: https://doi.org/10.58812/esiscs.v1i01.1121.

[8] K. Demertzis et al., “Communication Network Standards for Smart Grid Infrastructures,” Network, vol. 1, no. 2, pp. 132–145, 2021, doi: https://doi.org/10.3390/network1020009.

[9] Y. Muni, “A Review of Efficient Routing Architectures Using OSPF, BGP, and MPLS in Multi-Protocol Networks,” Eng. Technol., vol. 11, no. 01, pp. 8597–

8604, January, 2026, doi: https://doi.org/10.47191/etj/v11i01.21.
[10] B. Paul et al., "Heliyon Potential smart grid vulnerabilities to cyber attacks : Current threats and existing mitigation strategies," Heliyon, vol. 10, no. 19, p. e37980, 2024, doi: 10.1016/j.heliyon.2024.e37980.
[11] B. Pragathi and P. Ramu, "Authentication Technique for Privacy in Smart Grid Settings Safeguarding," E3S Web Conf., vol. 540, 2024, doi: https://doi.org/10.1051/e3sconf/202454010014.
[12] A. Ashok, A. Hahn, and M. Govindarasu, "Cyber-physical security of Wide-Area Monitoring, Protection and Control in a smart grid environment," J. Adv. Res., vol. 5, no. 4, pp. 481–489, 2014, doi: https://doi.org/10.1016/j.jare.2013.12.005.
[13] M. Angamuthu, R. Alazaidah, A. Shiney, D. Kirubakaran, V. Thrimurthulu, and V. Manasa, "Novel Cybersecurity and the Internet of Things (IoT) for Safeguarding Smart Grids: A Robust Architecture to Prevent Attacks on Specific Infrastructure," in 2026 9th International Conference on Circuit, Power & Computing Technologies (ICCPCT), 2026, pp. 2101–2107. doi: 10.1109/ICCPCT70290.2026.11654780.
[14] I. P. Member, M. Aghili, H. Riggs, A. S. Member, A. I. Sarwat, and S. Member, "A Novel Authentication Management for the Data Security of Smart Grid," IEEE Open Access J. Power Energy, vol. 11, no. October 2023, pp. 218–230, 2024, doi: 10.1109/OAJPE.2024.3393971.
[15] N. Saxena and B. J. Choi, "State of the Art Authentication, Access Control, and Secure Integration in Smart Grid," Energies, vol. 8, pp. 11883–11915, 2015, doi: 10.3390/en81011883.
[16] P. Patel, "Automated Detection of Insider Threats in Zero Trust Networks Through Machine Learning Techniques for Improved Security," in 2026 2nd International Conference on Artificial Intelligence Systems (AIS), San Antonio, TX, USA: IEEE, 2026, pp. 460–465, May. doi: 10.1109/AIS69919.2026.11621584.
[17] A. Algarni, "An Edge Computing-Based and Threat Behavior- Aware Smart Prioritization Framework for Cybersecurity Intrusion Detection and Prevention of IEDs in Smart Grids With Integration of Modified LGBM and One Class- SVM Models," IEEE Access, vol. 12, pp. 104948–104963, 2024, doi: 10.1109/ACCESS.2024.3435564.
[18] J. Chen et al., "applied sciences A Multi-Layer Security Scheme for Mitigating Smart Grid Vulnerability against Faults and Cyber-Attacks," Appl. Sci., vol. 11, no. 21, 2021, doi: https://doi.org/10.3390/app11219972.
[19] U. Rights, "Privacy - Preserving Technique in cybersecurity: Balancing Data Protection and User Rights," JCSTS, vol. 7, no. 3, pp. 248–263, 2025, doi: 10.32996/jcsts.
[20] Z. Dunya and M. Mazinani, "Cybersecurity in Smart Grids: Protecting Critical Infrastructure from Cyber Attacks," SHIFRA, vol. 2023, pp. 86–94, 2023, doi: 10.70470/SHIFRA/2023/010.
[21] G. Elbez, H. B. Keller, and V. Hagenmeyer, "A New Classification of Attacks against the Cyber-Physical Security of Smart Grids," in Proceedings of the 13th International Conference on Availability, Reliability and Security, in ARES '18. New York, NY, USA: Association for Computing Machinery, 2018. doi: 10.1145/3230833.3234689.
[22] A. D. Syrmakesis and C. Alcaraz, "Classifying resilience approaches for protecting smart grids against cyber threats," Int. J. Inf. Secur., vol. 21, no. 5, pp. 1189–1210, 2022, doi: 10.1007/s10207-022-00594-7.
[23] B. N. Jørgensen, "Cybersecurity and Resilience of Smart Grids : A Review of Threat Landscape , Incidents , and Emerging Solutions," Appl. Sci., vol. 16, no. 2, pp. 1–48, 2026, doi: https://doi.org/10.3390/app16020981.
[24] J. Li, "Fostering Resilience in Smart Grid Cybersecurity: A GAN-Based Synthetic Attack Data Generation Method for Imbalanced Intrusion Detection," in 2026 International Conference on Electrical, Control and Information Technology (ECITech), 2026, pp. 700–705. doi: 10.1109/ECITech69277.2026.11601246.
[25] K. Sultan, M. Ikram, and A. Rezk, "Probabilistic Trust Modeling and Security Verification for Smart Grid Systems," in 2025 IEEE PES Conference on Innovative Smart Grid Technologies - Middle East (ISGT Middle East), 2025, pp. 1–5. doi: 10.1109/ISGTMiddleEast65737.2025.11314277.
[26] S. Horbachenko et al., "Analysis and Optimization of Processes for Integrating Smart Grid Objects into the Critical Infrastructure Cyber Protection System," in 2025 IEEE 6th KhPI Week on Advanced Technology (KhPIWeek), 2025, pp. 1–5. doi: 10.1109/KhPIWeek61436.2025.11288406.
[27] O. V. G. Swathika, A. Karthikeyan, K. Rout, and S. Hatkar, "Cybersecurity Deployment in Smart Grids: Critical Review, Applications, Protection, and Challenges," IEEE Access, vol. 12, pp. 113618–113641, 2024, doi: 10.1109/ACCESS.2024.3443312.
[28] S. Simonthomas, R. Subramanian, and S. A. Mathiew, "A Survey of Enhancing Cyber Physical System Security in Smart grid," in 2024 International Conference on Communication, Computing and Internet of Things (IC3IoT), 2024, pp. 1–6. doi: 10.1109/IC3IoT60841.2024.10550307.
[29] A. Sharma and H. Babbar, "BoT-IoT: Detection of Attacks in IoT-Cybersecurity for Smart Transportation," in 2023 8th International Conference on Communication and Electronics Systems (ICCES), 2023, pp. 522–527. doi: 10.1109/ICCES57224.2023.10192814.
[30] M. Manbachi and M. Hammami, "Virtualized Experiential Learning Platform (VELP) for Smart Grids and Operational Technology Cybersecurity," in 2022 IEEE 2nd International Conference on Intelligent Reality (ICIR), 2022, pp. 54–57. doi: 10.1109/ICIR55739.2022.00027.