energies

MDPI

Review

Cybersecurity in Smart Grids and Other Application Fields: A Review Paper

Ahmad Ali [1,*], Mohammed Wadi [2] and Wisam Elmasry [3]

[1] Computer Science and Engineering Department, Istanbul Sabahattin Zaim University, Istanbul 34303, Türkiye
[2] Electrical Engineering Department, Istanbul Sabahattin Zaim University, Istanbul 34303, Türkiye; mohammed.wadi@izu.edu.tr
[3] Computer Engineering Department, Istanbul Kultur University, Istanbul 34158, Türkiye; w.elmasry@iku.edu.tr
* Correspondence: ali.ahmad@std.izu.edu.tr

Abstract

This article explores various applications and advancements in the fields of energy management (EM), cybersecurity (CS), and automation across multiple sectors, including smart grids (SGs), the Internet of things (IoT), trading, e-commerce, and autonomous systems. A variety of innovative solutions and methodologies are discussed, such as enhanced impedance methods for simulation stability, decision support systems for resource allocation, and advanced algorithms for detecting cyber-physical threats. The integration of artificial intelligence (AI) and machine learning (ML) techniques is highlighted, particularly in addressing challenges such as fault tolerance, economic distribution in cyber-physical systems (CPSs), and protection coordination in complex environments. Additionally, the development of robust algorithms for real-time monitoring and control demonstrates significant potential for improving system efficiency and resilience against various types of attacks.

Keywords: cyber security (CS); smart grids (SG); cyber protocols (CP); machine learning (ML); Internet of things (IoT); theories of defense and attack (TDA)

1. Introduction

The integration of the IoT and SG technologies has significantly improved EM, offering enhanced capabilities for monitoring, control, and optimization of energy distribution. The cybersecurity continues to be a topic of concern for researchers when applying the energy management systems (EMS) enabling bi-directional power flow and demand response for both residential and commercial buildings as identified as a potential challenge with EMS in [1]. These technologies enable real-time data collection, improving system efficiency, reliability, and sustainability. However, they also introduce significant CS risks due to the interconnected nature of IoT devices and SGs, which are vulnerable to cyber threats (CTs) that could impact national security, economic stability, and public safety.

This review examines the current state of CS in SGs and IoT systems, addressing the challenges posed by the diversity of devices, communication protocols, and security standards [2–5].The bidirectional communication between utility companies and consumers further complicates security efforts as shown in Figure 1. The risks of cyber attacks (CAs) on these systems are real, as demonstrated by incidents like the 2015 cyber-attack on Ukraine's power grid (PG) [6], which caused widespread outages [7]. The scientific community has responded with research focused on improving CS through threat detection, intrusion

Academic Editor: Michael Negnevitsky

Received: 16 September 2025
Revised: 28 October 2025
Accepted: 30 October 2025
Published: 1 January 2026

detection systems (IDS), encryption, secure communication protocols, and the use of ML and AI [8,9].

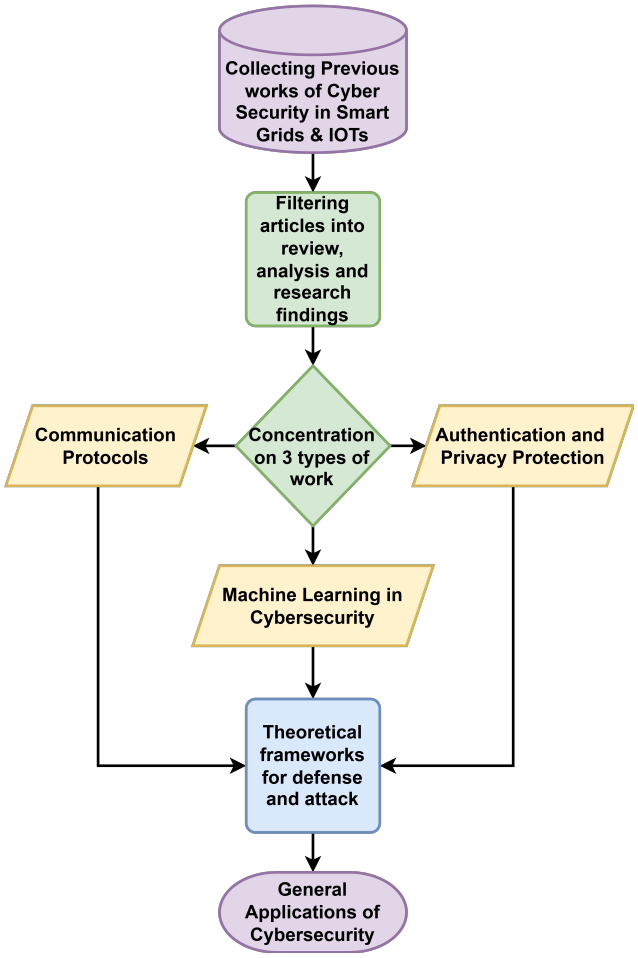

Figure 1. The Mechanism of Work.

During the ongoing conflict in 2022, Ukrainian energy infrastructure was again targeted by sophisticated cyber-attacks, including the "Industroyer2" malware, designed specifically to disrupt electrical substations [10]. Beyond conflict zones, energy providers globally face relentless threats. In 2023, a major Danish energy company, Orsted, was hit by a destructive ransomware attack, though it reported no operational impact due to robust contingency plans [11]. These incidents underscore that the cybersecurity challenges facing SGs are not only real but are continuously adapting, necessitating the ongoing research and advanced solutions discussed in this review.

This review research paper has been organized into six section as following:

1. Review, Analysis and Research Findings
2. Authentication Methods and Privacy Protection
3. Communication Protocols
4. Machine Learning in Cybersecurity
5. Theoretical Frameworks for Defense and Attack
6. General Applications of Cybersecurity

2. Methodology of the Review

To ensure a comprehensive, objective, and reproducible analysis of the literature, this review was conducted following a structured process inspired by the systematic review principles outlined in the PRISMA. The methodology comprised four main stages:

(1) Literature Search and Collection, (2) Screening and Selection, (3) Thematic Classification, and (4) Critical Synthesis and Analysis. 1. Literature Search and Collection: A systematic search was performed in three major academic databases: Scopus, Web of Science, and IEEE Xplore. The search was conducted to cover the most relevant decade of research, from January 2015 to 2025. 2. Screening and Selection: The initial search returned a total of 2318 records. After removing 347 duplicates, 1971 unique records underwent a two-stage screening process based on pre-defined inclusion and exclusion criteria:

- Inclusion Criteria: (i) Peer-reviewed journal articles; (ii) Primary focus on cybersecurity challenges or solutions in SG or IoT-based energy systems; (iii) Published in English between 2015–2025.
- Exclusion Criteria: (i) Papers not written in English; (ii) Short papers, editorials, or posters with limited technical content; (iii) Papers focused solely on physical security or non-cyber-related power system analysis.

In the first stage, the titles and abstracts of the 1971 records were screened, resulting in the exclusion of 1532 records that were clearly irrelevant. The remaining 439 full-text articles were assessed for eligibility. Of these, 224 were excluded with reasons (e.g., wrong context, insufficient technical depth, focus on non-energy IoT). This process yielded a final corpus of 215 primary studies that formed the basis for the in-depth review. 3. Thematic Classification and Analysis: The 215 selected papers were analyzed and categorized into six recurring thematic areas to structure the review:

1. Review, Analysis and Research Findings
2. Authentication Methods and Privacy Protection
3. Communication Protocols
4. Machine Learning in Cybersecurity
5. Theoretical Frameworks for Defense and Attack
6. General Applications of Cybersecurity

Within each theme, the findings, methodologies, and contributions of the papers were synthesized to identify trends, consensus views, research gaps, and future directions, as presented in the subsequent sections of this paper.

This methodology ensures a transparent and replicable process for evaluating the current state and future direction of SC in SGs and IoT environments. Figure 1 summarize the mechanism of our work.

Motivation of Research

The motivation behind this research is to address the increasing security threats (STs) to SGs and IoT systems, which are critical to the stability of modern energy infrastructure. The potential economic and social impact of cyber-attacks underscores the need for robust security measures tailored to these technologies.

Organization of the Review

This review is designed to provide a comprehensive and systematic exploration of CS in SGs and IoT systems. It is organized into several main sections:

- Review, Analysis and Research Findings: An overview of existing literature on CS challenges in SGs and IoT systems, highlighting current knowledge and research gaps.
- Authentication Methods and Privacy Protection: Examination of techniques for secure authentication and privacy protection within SGs and IoT environments, including various protocols and privacy-preserving methods.
- Communication Protocols: A review of communication protocols used in SGs and IoT systems, discussing their role in secure data transfer and suggesting improvements.

- Machine Learning in Cybersecurity: Focus on how ML and AI are applied to enhance CS, offering innovative methods for threat detection, response, and prevention.
- Theoretical frameworks for defense and attack: Exploration of theoretical models that guide cyber defense and attack strategies, including methodologies to predict and counteract CTs.
- General Applications of Cybersecurity: Broader discussion on applying CS principles across various SG and IoT contexts to enhance public security.

This structured approach aims to provide a thorough analysis of the CS landscape, offering valuable insights for researchers, practitioners, and policymakers focused on protecting critical infrastructure. Some works discussed as an enabling technology for the SG [12]. The main security challenges that IoT-based SGs could face are comprehensively surveyed [12,13].

3. Review, Analysis and Research Findings

This section summarizes research, scientific papers, review articles, and analyses of the most critical problems and solutions discussed in the field of CS in smart network (SN). In addition, other networks will be reviewed to benefit from them in collecting the most significant possible amount of appropriate content within this field [14–16].

A critical challenge in SG CS is the prioritization of limited defense resources against a vast landscape of potential threats. To provide a clear framework for readers and practitioners, a taxonomy for threat prioritization based on two key risk factors were proposed: Potential Impact (on grid safety, reliability, and stability) and Likelihood (the ease with which an attack can be successfully executed). This matrix, presented in Table 1, synthesizes findings from the reviewed literature to categorize common attack vectors and guide mitigation strategies. High-priority threats, such as FDI and coordinated DoS attacks, demand immediate and robust defensive measures due to their catastrophic potential and relatively higher probability.

The taxonomy presented in Table 1 is designed to synthesize findings from the reviewed literature into a practical framework for prioritizing cyber threats. The rankings for Potential Impact and Likelihood (Ease of Exploit) are based on a qualitative analysis of attack consequences and prerequisites, derived from consensus views in the academic and industry sources cited throughout this review. The scales are defined as follows:

- Potential Impact:
  - Catastrophic: Could cause widespread, prolonged blackouts (cascading failures), significant physical damage to critical equipment (e.g., generators, transformers), or pose a direct threat to public safety.
  - High: Could cause localized outages, substantial financial loss, major operational disruption, or a severe loss of situational awareness for grid operators.
  - Medium: Primarily causes financial fraud (e.g., energy theft), consumer distrust, or manageable operational inefficiencies.
- Likelihood (Ease of Exploit):
  - High: Attack leverages common, unpatched vulnerabilities (e.g., default credentials on IoT devices), uses widely available attack tools, or requires minimal knowledge of the specific grid topology.
  - Medium: Attack requires specific knowledge of the system (e.g., grid topology for some FDIAs) or access to more specialized systems (e.g., load control servers), but methodologies are documented in research.

– Low: Attack requires advanced, proprietary knowledge of the system, simultaneous compromise of multiple diverse systems, or sophisticated resources that are not readily available.

These criteria allow for a reasoned distinction between threat levels. For example, an FDI attack on state estimation is rated Catastrophic/Medium because its impact is potentially immense, but its execution requires specific topological knowledge, making it less likely than a simple DoS attack. This methodology provides a transparent basis for the prioritization that follows.

Table 1. A Taxonomy for Smart Grid Cyber Threat Prioritization.

Threat Category	Specific Attack Vector	Potential Impact	Likelihood (Ease of Exploit)	Priority Level
Data Integrity	False Data Injection (FDI) on State Estimation	Catastrophic: Cascading failures, blackouts, equipment damage.	Medium: Requires specific knowledge of grid topology.	HIGH
Data Integrity	Stealthy FDI (e.g., Ramping Attacks)	Catastrophic: Long-term, undetected degradation of grid stability.	Low: Requires advanced knowledge and access.	MEDIUM-HIGH
Availability	Coordinated DoS on Critical SCADA/PMU Links	High: Loss of situational awareness, inability to control, localized outages.	High: Many existing vulnerabilities in protocols and devices.	HIGH
Availability	Load Redistribution Attack (LRA)	High: Can trigger line overloads and cascading failures.	Medium: Requires access to load control systems or AMI.	HIGH
Availability	Ransomware on Utility IT Networks	Medium-High: Financial loss, operational disruption, data theft.	High: Common attack vector with many entry points (e.g., phishing).	HIGH
Ecosystem	EV Charging Station Compromise (Session Hijacking)	Medium: Financial fraud, consumer distrust, localized load spikes.	High: Many consumer-grade chargers have weak security.	MEDIUM
Ecosystem	Fleet-wide EV Charging Coordination Attack	High: Significant, sudden grid imbalance (Demand-Response Attack).	Low: Requires compromising multiple, diverse systems.	MEDIUM
Authentication	Compromise of Default Credentials on Field Devices	Variable: Can be a first step to a high-impact attack (e.g., FDI).	Very High: Still prevalent in legacy and some new devices.	MEDIUM-HIGH

Various attempts and incidents in past years have implicated phase measurement units (PMU) [17], digital fault recorders, intelligent electronic devices, supervisory control and data acquisition (SCADA), cyber communications components, and advanced measurement infrastructure (AMI), all of them are vulnerable to CAs. They must be protected against hacks and CAs.

Rajaa Vikhram Yohanandhan et al. [18] studied Cyber Physical Power System (CPPS) networks and found that their heterogeneous nature necessitated conducting multidisciplinary tests to evaluate new CAs and discover vulnerabilities and threats to CPPS. Using this CPPS testing framework, it can detect different types of CAs and evaluate the detection algorithm used, which in turn helps develop sustainable CS defenses for the CPPS environment. They reviewed the CPPS test layers from different angles, such as the physical PS layer, communication layer, sensor layer, application layer, control layer, test platforms, and research objectives with the integration of cyber and physical systems. They also reviewed the physical power infrastructure of CPPS, CPPS protocols, communications networks in CPPS, Cloud Computing (CC) and data analytics, software tools for modeling and simulation of CPPS, CAs in CPPS, failure cascade analysis of CPPS, CS and privacy

in CPPS, and resilience and reliability analysis of CPPS. They provided an overview of CPPS networks, architecture, assessment, and description of the necessity of CA testing and sustainable CS analysis in CPPS [19]. Figure 2 gives a quick overview of the classifications of cyber attacks in smart grids.

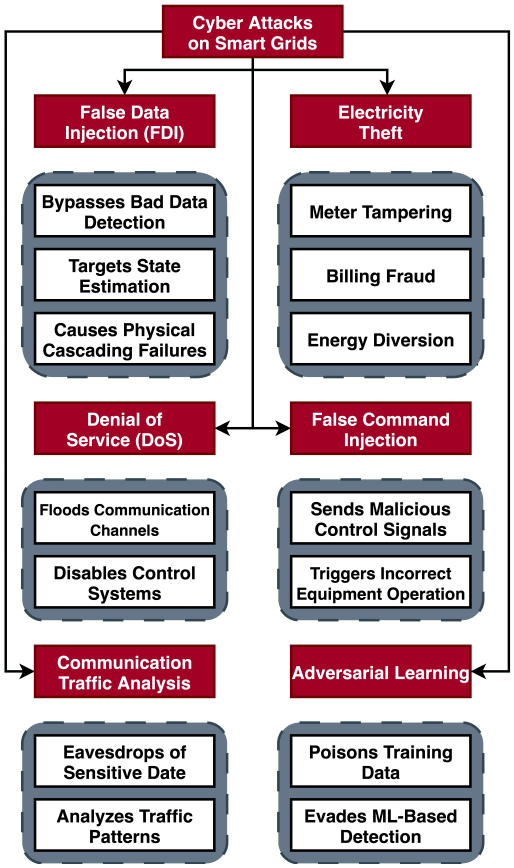

Figure 2. Classifications of cyber attacks in smart grids.

Based on the analysis of ubiquitous electric IoT network development trends and technical requirements, another work proposes smart meters (SMs) and suitable acquisitions of SG information acquisition systems in addition to a lightweight two-way device authentication protocol [20]. The protocol is based on two main elements: a shared security key and random numbers to verify the identity of both parties to the communication. They proposed using the security key embedded in the device chip to determine the legitimacy of the identity of the access device, avoiding the use of third-party services such as certificates, and effectively preventing frequent man-in-the-middle attacks. Some experiments have shown that the time for lightweight XOR data decryption is 1/2 the time of a typical Data Encryption Standard (DES) algorithm and 1/900 the time of an Rivest–Shamir–Adleman (RSA) algorithm. The obtained efficiency was much better than DES and RSA, which is consistent with industrial control systems (ICSs). They collected possible general incident patterns and worked out CA classifications and application scenarios for ubiquitous energy IoT network attacks.

In [21,22], the performance effects of False Data Injection (FDI) attacks on cascading failures of a CPPS were studied through a set of steps: First, the power flow characteristics of the power network and the monitoring and control functions of the cyber network were taken into account. Second, a proposed model of the energy CPS was created. Third, the false data attack (FDA) and its impact on decision-making processes and control of communications operations in the cyber network were studied. Fourth, a successive failure analysis process for the CA environment was proposed. Fifth, an indicator was

proposed to evaluate the network's vulnerability from two perspectives, the first of which is the operating characteristics of the power network and the second of which is the structure's integrity.

A dynamic Bayesian game-theoretic approach is proposed to analyze FDI attacks with incomplete information [23]. In this approach, according to a proposed bi-level optimization model, players' payoffs are identified, and based on history profiles and relationships between measurements, the prior belief of the attacker's type is constantly updated. It is proven that the type belief and Bayesian Nash equilibrium (NE) are convergent. By the law of large numbers and the central limit theorem, the stability and reliability of this approach can be guaranteed. By using the dynamic Bayesian game-theoretic approach, the defender can efficiently allocate resources to at-risk load measurements [24].

Jinsoo Shin et al. [25] investigated safety and security perspectives when conducting risk analysis for nuclear facilities by adopting the System-Theoretic Process Analysis (STPA)-SafeSec methodology to know the impacts on safety through CAs against digital information and control systems. They applied this methodology to a test bed system that simulates a condensing water system in a nuclear power plant (NPP). They described the development of mitigation strategies and the implementation process in detail.

A. Vaccaro et al. [26] analyzed the enabling methodologies related to SG computing, monitoring, and control. Accordingly, they proposed research into designing more flexible and scalable solution models based on decentralized, comprehensive, proactive, and self-organizing computing. This, in turn, is reflected in strengthening the procedures for operating sensor networks (SNs) and developing their work with a set of information services that help discover knowledge and extract data.

In [27], all the standards required by CS that were actually applied to SNs were collected and identified. Based on these reviews, seventeen criteria were described and identified. Additionally, focus was placed on SC requirements and related evaluation criteria [28]. The relationships between the standards were also analyzed and studied to identify points of overlap in the standards and points of independence.

A valuable review of SGs considering wireless communications technologies (WCTs) comprehensively reviewed [29,30]. Different network attributes were studied to compare communication technologies in the context of an SG, such as Internet Protocol support, power usage, data rate, etc. taken into consideration. They also discussed some technologies, such as 6LoWPAN, Wi-Fi, Bluetooth, ZigBee, and Z-Wave, which are suitable for Home Area Networks (HANs). They then compared these technologies in the context of network characteristics and consumer interests. Also, in the context of public utility concerns for WCTs for Neighborhood Area Networks (NANs), a similar approach was adopted, including cellular standards based on GSM and Worldwide Interoperability for Microwave Access (WiMAX).

In another work [31], they addressed and analyzed the problem of FDI attack, where they found that this attack can bypass bad data detection mechanisms in estimating the state of the power system (PS). They worked to distinguish between the attack and normal patterns to propose an unsupervised method.

Sandeep Pirbhulal et al. [32] conducted a study aimed at conducting a comprehensive systematic literature review on the subject of developing techniques, protocols, methodologies, RAMS analysis tools, and models for various applications. They collected 1513 records that were published between 2011 and 2020. A comparative analysis of existing solutions has been done based on various aspects such as developed methodologies and architectures, targeted applications, implementation scenarios, performance evaluation mechanisms, protection aspects of applied Critical Infrastructures (CIs) associated with RAMS, and pros

and cons. They show that RAMS analysis of CIs with applications such as CC, PG stations, maritime transportation, CPSs, and ICSs is an emerging research area.

In [33], the information security (IS) threats facing the Energy Internet were reviewed. Then, the flaws in these networks were classified, and ways to protect the security of information related to power plants were studied. According to the network security characteristics, the research also studied the system architecture of the distributed power station in the energy Internet environment, analyzed the counter-protection measures to protect the IS of such stations, and worked to build a network security framework for these stations and to analyze and provide the IS of the distributed power station [34].

In [35], a hybrid framework based on a physical model was proposed to estimate non-technical power losses in distribution networks. Non-technical energy loss is defined as energy received by the consumer but not invoiced. Contemporary solutions to this issue typically utilize either data-driven approaches or physical models. However, data-based solutions alone have proven inadequate, necessitating the adoption of analytical solutions grounded in physical models.

Engineering assessments and expert judgments are among the methods for assessing cyber risks [36]. One of the difficulties facing these assessment methods is that no database is available for NPPs containing potential CTs. Therefore, they adopted operational experience analysis to estimate the frequencies of CTs. First, they grouped running experiments according to their characteristics to propose a list of CTs. Second, through Bayesian updates, the frequency of each CT is calculated in two stages.

Mohab Aly et al. [37] presented an interesting article on understanding IoT security issues. They comprehensively described the security challenges and threats facing networks across the different layers of the IoT systems architecture [38]. They then presented countermeasures and proposed solutions to these security challenges and threats.

Refs. [39,40] presented another method for assessing SC risks, which includes new communications concepts, information technology, and old systems. Two paths of analysis can be used to identify risks associated with the architectural concept of the SG. The first is an analysis at the conceptual level that attempts to understand the risks to which SG components cannot be implemented. The second is an implementation-level analysis that works on current prototypes and legacy systems and shows their role in the candidate SG architecture.

In [41], a comprehensive review of the most significant research works in SNs, focusing on IoT applications, was conducted. The review highlighted numerous innovative methods in SNs and the IoT and discussed their applications across various fields.

In [42], the role of sonification and its usefulness in a network traffic sonification system to represent network attacks was analyzed and evaluated. In this system, data was represented as sound. Accordingly, network security information and network attacks were converted into audio signals. The results showed that participants could accurately and efficiently detect attacks by listening to audio network data and could even identify types of attacks.

In [43], classification and identification of weak and critical links of traffic networks, two new methodologies based on the Fisher information matrix, eigenvectors and eigenvalue analysis, were presented to identify and classify weak and critical links of traffic networks. Traffic variables, such as network flow and travel time, are used to identify.

In [44], an analytical formula was presented to evaluate system reliability in SGs based on the availability of the central remote control system and the impact of the weakness of the CPS. It is expected that the protection system will be developed towards the use of remotely controlled circuit breakers, which in turn will help overcome this weakness

and move towards a CPS that works according to protection schemes based on remote-controlled switches.

In [45], a comprehensive summary of CAs targeting ICSs and approximately forty-three attacks that caused severe damage to critical national infrastructure was provided. They documented previous ICS-focused CAs, analyzed them, and documented their evolution to understand better the threat actors, attack vectors, and targeted sites and sectors. A reliability assessment technique for CPPSs in the field of SC was presented in [46]. The technique is based on analyzing non-normal random variables with non-linear dependencies. Bidirectional Encryption Representations from Adapters were used to analyze their textual description and predict the severity of cyber vulnerabilities. This model allows manual text entry describing threats to predict the probability of cyber vulnerability. A Bayesian attack graph was used to simulate attack paths. A Markov model was used to explain the consequences of CAs.

In other analytical research, they analyzed and evaluated the SC risks associated with aggregating distributed energy resources (DER) or an edge device and developed an approach that limits or mitigates these risks [47]. In [48], a method for monitoring a connected network's managed security measure, the Seamless Security Application Method, was presented. The advantage includes the lifespan of managed security measures by checking and exploiting vulnerability levels. The case-based analysis process adapts Q-learning to identify and update the case and work on the necessary security measures. This procedure provides continuous support for operating applications and reduces premature termination of the security procedure, which reflects positively on the efficient exploitation of sustainable energy resources.

In [49], a comprehensive solar Photovoltaic (PV) technology comparison of four decision tree (DT) algorithms for static security evaluation and classification was performed using the C4.5 approach. A four-step process was proposed to build a binary classifier: selecting the best classifier and evaluating performance, data collection, technique comparison, pre-processing, and feature selection. The study was applied to five (5) photovoltaic power generators producing a total power of 40 MW on the IEEE 30 bus system.

In [50] discusses criteria for evaluating SG SC. The results of the systematic analysis were presented by identifying criteria that provide sound guidance for a security assessment to solve the problem of the presence of many criteria and the inability to combine them. This study showed that there are six criteria for SG or energy systems that provide security assessment and can be applied to substations, IACS, or all SG components.

The hostile goals of attackers: firmware modification attacks through which attackers attempt to switch and control input modification attacks targeting the microgrid (MG) system using inverter-based distributed generation (DG) were analyzed [51]. The use of hardware performance counters with time series classifiers has been proposed.

In [52], a framework was proposed to model the SG as complex interconnected networks, and then the structural weaknesses that could be vulnerable to attacks were investigated. These attacks are considered a severe electronic, physical threat. One type of FDI attack is a load redistribution attack (LRA). A new approach was presented to identify cascade attack targets based on the intelligent attack mechanism and the node's importance, as the attack can lead to the collapse of the entire PS [53]. The effectiveness of the proposed strategy was verified on the IEEE 39 bus and the actual district core network.

In [54], a bibliometric survey of research papers on the security aspects of SGs supported by the IoT was presented. This survey concludes that SG systems' complexity and threats' diversity call for intelligent and comprehensive security approaches. The survey also expects future publications to focus on increasing the computational speed of security algorithms with a low rate of false alarms and maintaining high detection accuracy. The

survey also revealed a research gap: most research papers focus on detecting CTs and how to prevent them. However, few focus on mitigating the CTs that affect SGs.

Ref. [55] presented a comprehensive review of vulnerabilities identified in distribution substations, particularly from the attacker's perspective. It delineated the vulnerabilities that potential attackers could exploit and subsequently discussed countermeasures against these CAs. The key elements necessary for a comprehensive SC solution for electrical substations were also identified.

The modern SG is evolving beyond a traditional, centralized grid into a complex Cyber-Physical System (CPS) that deeply integrates Distributed Energy Resources (DERs), Electric Vehicles (EVs) and their charging infrastructure, and smart buildings. While this integration enhances flexibility and sustainability, it profoundly reshapes the cybersecurity landscape by dramatically expanding the attack surface and introducing novel vulnerability vectors [56].

Expanded Attack Surface through Interdependencies: The interconnection of previously isolated systems creates a web of cyber-physical interdependencies. For instance, an attacker compromising a cloud-based platform managing a fleet of DERs can inject false data to cause local voltage violations or frequency instability [56]. Similarly, EV charging stations, particularly public and residential "smart" chargers, represent a massive and often poorly secured entry point. A coordinated attack on a fleet of EVs (a "Demand-Response Attack") could be orchestrated to simultaneously start drawing high power, creating a significant, sudden load on the distribution grid that could trigger instability or even blackouts [57]. The compromise of one system component (e.g., an EV telematics unit) can thus serve as a pivot point to attack the broader energy infrastructure.

New Vulnerabilities from Bidirectional Data Flows: Integration is enabled by continuous, bidirectional data exchange. Unlike traditional one-way meter reading, integrated systems rely on two-way communication for functions like vehicle-to-grid (V2G) services, where EVs feed power back to the grid. This creates new attack vectors. For example, False Data Injection (FDI) attacks can manipulate pricing signals or control commands sent to DERs and EVs, leading to inefficient energy dispatch, financial fraud, or physical damage. Furthermore, the privacy risks are magnified; detailed consumption data from EVs and smart inverters can reveal sensitive information about user behavior and occupancy patterns.

Zhang et al. [57] further elaborate on the cyber vulnerabilities of EV battery chargers, discussing both attack impacts and latest hardware/software-based detection techniques. Securing this integrated ecosystem requires a holistic approach that moves beyond protecting the core grid to encompass the entire supply chain of connected devices and the communication protocols that bind them together.

4. Authentication Methods and Privacy Protection

In this section, there will be a brief review of the works and research that dealt with the topics of authentication approaches and privacy protection in protection systems in general and SC in particular, with their applications in SNs and others. Table 2 summarizes authentication approaches and privacies, the table also includes methods involving secure key management (KM), blockchain (BC)-based solutions, lightweight authentication protocols, intrusion detection, and privacy-preserving mechanisms applied in various domains such as healthcare, CC, and smart homes (SHs). Each entry summarizes the major contribution, output, and year of publication, offering a broad insight into the latest trends and solutions in the field. Zhitao Guan et al. proposed a solution to the problem of trading based on BC technology, as most face the problem of privacy disclosure [58]. They proposed ciphertext Policy Attribute-Based Encryption as the basic algorithm for reconstructing the transaction

model. This idea works by building a public model for distributed transactions called PP-BCETS (Privacy Preserving BC Energy Trading System). Arbitrating transactions in the ciphertext form can achieve fine-grained access control. In this way, the protection of private information can be increased, and the reliability and security of the transaction model can be greatly improved.

In another work, an SC-assisted authentication method for SGs is proposed to overcome the flow of false data [59]. This method relies on estimating the energy requirements of the meters in advance based on information obtained previously. Then, according to these previously provided parameters of the distribution method or rated power requirement, authentication-based security is provided. At the same time, the monitoring process continues for differences in SG data to allocate power based on the network and end-user consumption at the current time of connection. Thus, power distribution is enhanced without stagnation or overload. In [60] examined the issue of application layer protocols for the IoT, as these protocols are considered by their nature not equipped with sufficient security guarantees, such as the Message Queue Telemetry Transport Protocol and the Constrained Applications Protocol [61]. Then, they proposed a solution suitable for critical IoT-based applications: a three-factor authentication framework based on a digital signature, identity, and password system. This framework takes advantage of Elliptic Curve Cryptography (ECC) and computationally low hash chains because it uses the publish-subscribe pattern. The results have proven that this framework resists different types of cryptographic attacks. They used the Scyther tool to perform automated verification of any of these requirements to ensure no cryptographic attacks in the proposed framework on any of the mentioned claims. For further discussion on ECC-based communication protocols, please refer to Section of Communication Protocols.

Table 2. Cyber security in the Smart Grid: Authentication.

Work Area	Summary	Ref.	Year
Smart PGs Capabilities	Critical SG challenges surveyed	[30]	2016
CPS Security	Risk assessment, Physical Unclonable Function (PUF) role	[14]	2017
Fog-based SCADA	IDS classification, privacy/authentication review	[62]	2020
Device Authentication Protocols	Lightweight mutual authentication using keys	[20]	2020
User Authentication	Authentication based on energy need; improves false data detection	[59]	2021
ECC-based Framework	3-factor Authentication using identity, password, and digital signature	[60]	2022
ITS Privacy	PC switching using CPC improves pseudonym changes	[63]	2023
SG Key Services	Smart scheduling, attack surface control with executor mgmt	[64]	2021
Anonymity in Authentication	Group blind signature and HE for integrity	[65]	2020
ECC Mutual Authentication	Lightweight ECC system with session key phase	[66]	2021
Key Agreement	Anonymous, lightweight AK protocol for DR	[67]	2021
BC Keyless Sig.	Decentralized keyless sig. via BC, secure access control	[68]	2019
Fission Computing	Trust/privacy via edge-crowd model	[69]	2019
EPPS in AMI	FDIA resistance via GMM and MSE-based learning	[70]	2021
ICS Networks	Steady-state CPS correction under attacks	[71]	2021
Security Frameworks	SMG in MICIE & CockpitCI bridges CS and control theories	[72]	2018
Hybrid MGs	Modified SCA + BC for AC-DC trading	[73]	2021
Authentication in SG Net.	Lightweight AK protocol, no key escrow, random oracle-secured	[74]	2021
RFID Security	Lightweight RFID Authentication for IoT, ensures secrecy	[75]	2018
IoT + Cloud Authentication	Lightweight cloud-Authentication for IoT with minimal overhead	[76]	2019
FDI Protection	MILP model for blackout-aimed cyberattack detection	[77]	2021
Bidirectional DB	Enhances query speed and reduces attack vector	[78]	2018
SCADA Vulns	Access control model derivation method	[79]	2021
IoT-Wireless Authentication	Secure AK protocol for WSNs; improves smart card handling	[80]	2019
W3C-Prov Authentication	Standardized model unifies all Authentication factors	[81]	2017
IEC 62351 Fix	Secure protocol using hash + key; avoids GOOSE/SV issues	[82]	2020
Cloud Authentication	Improved cloud-SM Authentication via TA	[83]	2020
IoT Smart Cities	Trusted sensing model using digital certificates	[84]	2023

Table 2. *Cont.*

Work Area	Summary	Ref.	Year
DRN-KeyGen	DL-based Authentication for LTE IoT; re-Authentication with low overhead	[85]	2024
BC IoT Authentication	BlendCAC for smart contract-based access control	[86]	2023
RFID-SAM	SAM protocol boosts tag-read Authentication	[87]	2020
Gesture Authentication	Gesture typing on mobile; superior features	[88]	2019
Authentication Techniques Review	Review of total Authentication methods (SFA & MFA)	[89]	2018
BC SH	BC + fog solves cross-domain Authentication	[90]	2024
Healthcare IoT	LMDS-based secure medical IoT Authentication	[91]	2021
Activity-Based Authentication	User Authentication via activity sensor patterns	[92]	2018
Roaming Authentication	Lightweight Authentication with session keys	[93]	2024
IoD Security	Lightweight protocol using dynamic IDs	[94]	2023
Fog-IoT Authentication	Multi-factor scheme using BC + light-chain	[95]	2024
Mag-PUFs	Electromagnetic Authentication with MAG-PUFs	[96]	2024
PUF in Med-IoT	GIFT-COFB + PUF for secure SHS	[97]	2024
LoRaWAN	MAB-based resource allocation	[98]	2024
Post-Quantum Authentication	Post-quantum secure Authentication for cloud health apps	[99]	2024
Vehicular Cloud	A3C+Dropout model for delay/energy reduction	[100]	2024

In [63], they examined the issue of data transfer in cooperative intelligent transportation systems, where users' privacy must be protected, especially when their locations are hidden, and every message must be authenticated. Authentication is done by signing messages with a private key associated with a pseudonym certificate provided by a trusted authority (TA). For the recipients to authenticate the messages, a computer is delivered with the messages, and to ensure privacy and protection from trackers from obtaining information regarding the drivers' locations, for example, computers are changed several times during the trip. So, in this work, they proposed a new method to manage computer switching intervals between vehicles. The method relies on having a shared computer as an intermediary before switching to a new computer. So that all vehicles use this shared computer to sign their messages during this period. Other work examined the topic of edge computing and the security and risks it can bring to the SG [64]. They proposed a heterogeneous polymorphic security architecture (SA) for edge-enabled networks. The proposed architecture provides intelligent executor scheduling based on dynamic heterogeneous redundancy architecture, attack surface management, executor cleaning and rebuilding, and intelligent arbitration of multi-instance service response. Figure 3 shows the layered security architecture for SG CS. To decide, modify, process, schedule, migrate, clean up, rebuild, and recover, they created a closed-loop core control process. To solve the problem of unidentifying the malicious user in the case of anonymous authentication (AA) and to achieve conditional anonymity, a collective blind signature system in the SG is proposed in [65]. It takes place in four stages: First After the CC creates the system parameters, the SMs and Security Servers (SSs) finish the registration. Second: Using the Schnorr ID, the SMs authenticate anonymously with the SSs, and with the SMs to verify the integrity of the data, homogeneous tags are created. Third, A blind signature of the group is generated by the SS for the data from the authenticated SM. Fourth, The integrity of the data and the validity of the signature are verified by CC. Threats facing the SG include CTs to send messages, network control, and information, and the possibility of harming consumers' privacy in the SG environment were studied in [66]. One of the solutions provided for these threats is to establish a secure connection between the consumer and the service provider (SP) and perform Mutual Authentication (MA) between them. In another work, a MA scheme was proposed based on elliptic curve encryption of substations and consumers with simple operations for a SG environment to protect them from STs. One of its advantages is that it provides a significant negotiation phase for the session, reflecting positively on providing a secure connection and reducing communication costs.

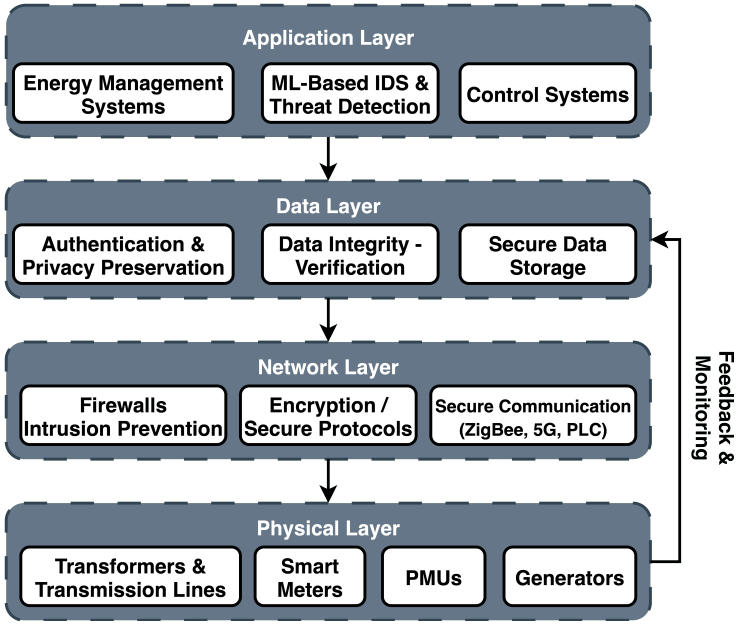

Figure 3. Layered Security Architecture for Smart Grid Cybersecurity.

Also, a trusted and secure key agreement system is crucial in SNs, and various studies have been done in this regard [67]. In this work, a protocol is proposed to address the limitations and drawbacks of a previously proposed protocol. The proposed protocol is a lightweight, anonymous, authenticated key agreement for intelligent network-based demand response management. Its features are that it supports privacy, withstands various security attacks, and supports MA. The proposed protocol was tested using automated ProVerif simulation and Burrows Abadi Needham logic analysis. KM between SPs and SMs is crucial in SGs [68]. This is done by trusted third parties but becomes insecure if the Trusted Third Party (TTP) fails. Since the providers of these services are centralized, there is a single point of failure. This paper proposed a decentralized keyless signing scheme based on BC consortium to achieve more secure and efficient KM. Using the BC network for data transfers, the SM sends requests and receives responses. A secure, decentralized consensus mechanism is designed to turn the BC into an automated manager that does not require a TTP or trust anchor, which controls access. SPs can also monitor each other using BC according to the proposed model. In a similar area, trust and privacy in Social IoT are essential for operating and exchanging information with edge devices [69]. Current solutions rely on a single central server and a trust scoring system. These registration systems are vulnerable to tampering. So, this work proposes a new approach in the form of fission computing. The proposed approach relies on edge integration with the crowd to maintain privacy rules in S-IoT and maintain trust. This is done by modeling entropy to determine trust between entities and using crowdsourcing as mini-edge servers. Fission Managers are responsible for maintaining the privacy rules for each S-IoT application. Another work proposed an "End User Privacy Protection System" [70]. The system enables SMs to report the correct reading during an False Data Injection Attack (FDIA) [101,102]. In this proposed technique, the actual measurement secret interval against FDI and data protection capability are evaluated based on the statistical ML method by clustering mean square error and Gaussian mixture models (GMMs). In [71], the control transformation strategy for the physical information network was analyzed and studied in light of the dynamic data attack (DA) in the ICS. A relevant mathematical model of CPSs was created for analysis to stabilize the CPS. An innovative algorithm has also been proposed to correct the steady state of CPSs to achieve good control performance under the dynamics of DAs.

This is done by successfully transforming the problem of system stability into the problem of control strategy flexibility.

In Industrial Control and Automation Systems, other research has examined security challenges that require evaluating security strategies and new risk assessment [72]. To respond to threats promptly and manage vulnerabilities properly, a security framework and advanced tools have been proposed. This strategy has been implemented in the ATENA architecture, designed as an innovative solution for protecting critical assets. An initial version of the secure brokerage gateway was designed in the Mission Critical Information Infrastructure Protection (MICIE) project and optimized in the CockpitCI framework. Even in grid-connected hybrid AC-DC MG systems, the systems also need to achieve safety and reliability since any changes in them can affect the power management of the entire system. So, in further research for power management of the entire system, the modified sine cosine algorithm was developed [73]. In addition, BC technology has been used to increase the security of energy trading within these hybrid MGs connected to the AC-DC grid. Random convection flow, based on copula mode, was used to create a realistic model. An SG key agreement protocol and a lightweight AA key for SG communications are proposed [74]. A security analysis was presented based on the random oracle model, which proved the security of the proposed protocol. The security of the proposed protocol was verified using a tool from the AVISPA program. Some security features of this proposed protocol have been proven, such as message authentication, replay attacks, SP anonymity, man-in-the-middle attacks, anonymity, impersonation attacks, key freshness, session key agreement, and non-traceability; in addition, communication and accounting costs are much lower. In RFID-based authentication systems, many authentication systems are designed using lightweight cryptographic tools [75]. Many of these designs fail to meet the required safety and functionality requirements. Another research has presented an authentication architecture for RFID-based IoT applications for future smart city (SC) environments. Then, a lightweight authentication scheme was introduced to provide a more reasonable implementation time than existing schemes based on RFID. This system features forward secrecy, RFID tag untraceability, anonymity, and secure translation. A new authentication scheme is proposed for IoT-enabled device-based environments combined with cloud servers [76]. They adopted lightweight encryption modules to achieve the best efficiency. Examples of cryptographic modules that have been adopted include one-way and exclusive hash functions or run. The advantage of this proposed system is that it is suitable for resource-limited environments, such as IoT devices or sensors, and one of its advantages is that it removes the computation burden. Proverif has verified its effectiveness. To confront CAs that cause power outages in large-scale networks and target bypassing multiple transmission lines, a bi-level mixed integer linear programming model was developed to accurately model FDIs [77]. It has been demonstrated that an FDI attack can be detected using a detection framework based on weighted least squares (WLSs) estimation instead of classical WLS estimation.

In the context of data, it is necessary to talk about a two-way data transformation methodology with common language data representation to overcome updating problems related to data and metadata. The updated information has different data types and formats. It thus reduces the ability of devices and databases to prepare to investigate the information due to this difference and lack of similarity. A new approach was presented that allows data to be mapped and helps to understand their differences at the level of data representation [78]. This mapping is made using Extensible Markup Language (XML)-based data structures as an intermediate data provider. Using XML, data can be converted bidirectionally from traditional data format and Resource Description Framework without data loss and with improved remote data availability. The vulnerabilities and STs of the

SCADA system are discussed, with a comprehensive methodology proposing appropriate security mechanisms [62,79,103]. The methodology is based on extracting the appropriate structure after defining security policies and models, identifying security needs and objectives, and implementing security mechanisms that protect against risks and meet needs. A new access control model named CI-OrBAC has been proposed. Stream Control Transmission Protocol (SCTP) was proposed as a transport protocol between the control and command planes. The Hash-Based Message Authentication Code (HMAC) field included in the ModbusSec message verifies hardware authentication and data integrity in the area between the control and command planes [104]. An evaluation of lightweight two- or three-factor authentication protocols showed that they are weak to strong replay attacks and do not provide complete confidentiality [80,105]. Therefore, a key agreement protocol for wireless sensor networks (WSNs) and secure and lightweight IoT-based authentication is proposed. A simulation of the proposed protocol was performed using the AVISPA tool to verify the security. The results show that the proposed protocol is secure against active and passive attacks. Other work within this context focuses on notions of pragmatic social validation based on the nature, quality, and length of prior encounters [81]. Using previous interactions, the basic similarity of the authentication factors is determined. Based on the W3C Provenance Working Group model, a unified representation model of secure interaction resources is presented. The paper also presents formal security proposals for defining secure interaction source schemes. A fuzzy control logic was implemented for the interaction source logs to create a new authentication and threshold-based access control model. The research also presents a protocol for registering and authenticating the interaction source and implementing the proof of concept.

Bera and Sikdar have proposed a security protocol for post-quantum communications in SG applications that ensures resilience against both classical and quantum attacks [106]. In [107], Gharavi et al,. have looked at the different types of PQC and their recent standard primitives to determine whether they can enable security for BC-based IoT applications. This study shows how post-quantum BCs are being developed and how it can be used to create security mechanisms for different IoT applications. And also, this study explores the main challenges and potential research directions that arise from integrating quantum-resistance BCs into IoT ecosystems. In [108], Najet Hamdi proposes a FL-based intrusion detection for SCADA systems where clients have different attacks. The impact of having missing attacks in local datasets on the performance of FL-based classifier were classified. Also, a hybrid learning method that combines centralized and federated learning was proposed. Lazzarini et al., evaluate the use of federated learning (FL) as a method to implement intrusion detection in IoT environments. When compared against a centralized approach, results have shown that a collaborative FL IDS can be an efficient alternative, in terms of accuracy, precision, recall and F1-score, making it a viable option as an IoT IDS. Additionally, the alternative aggregation algorithms, namely FedAvgM, FedAdam and FedAdagrad were evaluated in same settings. The results show that the FedAvg and FedAvgM tend to perform better compared to the two adaptive algorithms, FedAdam and FedAdagrad [109]. Alqahtani and Kumar comprehensively explores cybersecurity challenges, including cyber-physical threats, privacy vulnerabilities, and supply chain risks and investigates artificial intelligence (AI)-driven solutions to bolster EnFV cybersecurity. The study begins with an overview of EnFV cybersecurity issues, emphasizing the increasing complexity of threats in digital transportation systems [110]. Ronanki and Karneddi provide an overview of the latest research contributions regarding the evolution of battery charger architectures, control methods, EV supply equipment (EVSE), charging protocols, communication channels, and their compliance from the perspective of cyber security. Furthermore, the potential impacts of sabotage cyber-attacks on various popular battery

chargers are explored. In addition, the latest hardware and software-intensive cyber-attack detection and countermeasure techniques are discussed [111].

While blockchain technology offers a decentralized and tamper-resistant ledger ideal for applications like energy trading and access log auditing, its adoption in SGs faces significant practical barriers that are often understated. The core operational requirements of a SG frequently conflict with the inherent characteristics of many blockchain implementations.

First, the issue of high latency is paramount. Consensus mechanisms, particularly Proof-of-Work (PoW), can require several minutes to achieve transaction finality. This is incompatible with real-time grid operations such as frequency regulation, fault protection, or even rapid demand response, which require decision-making in milliseconds to seconds.

Second, the energy consumption of PoW-based blockchains is substantial, creating a paradoxical situation where securing the grid's data transactions consumes an excessive amount of the very resource the grid manages. Although alternative consensus mechanisms like Proof-of-Stake (PoS) are more energy-efficient, they often introduce other trade-offs like potential for centralization.

Finally, scalability limitations present a major hurdle. Throughput in large, permissionless blockchains is typically limited to tens of transactions per second, while a fully deployed AMI with millions of SMs can generate a continuous, high-frequency stream of data points. Storing every meter reading on-chain is currently impractical and prohibitively expensive.

Therefore, blockchain is not a one-size-fits-all solution. Its application is best suited for non-real-time, high-value transactions where decentralization and auditability are critical, such as settling financial energy trades between utilities, managing renewable energy certificates (RECs), or maintaining tamper-proof logs of critical configuration changes. For real-time control and massive data collection, hybrid architectures or alternative technologies are more appropriate.

While the surveyed authentication schemes show significant promise, several challenges remain for widespread SG deployment. Lightweight cryptographic protocols often face a trade-off between security and functionality, sometimes sacrificing perfect forward secrecy for reduced computational overhead. Blockchain-based solutions, as discussed in this Section, difficulties with scalability and latency. Furthermore, many proposed schemes are validated in isolated testbeds and lack evaluation under real-world SG constraints, such as network congestion during fault conditions or the presence of legacy devices that cannot be easily upgraded. A key unresolved issue is the development of agile authentication frameworks that can dynamically adapt their security parameters based on real-time threat levels without disrupting grid operations.

5. Communication Protocols

This section provides a review of research publications that focus on communication systems in SNs. It includes reviews of the most notable systems employed and an analysis of their advantages, disadvantages, and the issues they encounter. Figure 4 illustrates cyber-physical attack & defense framework in smart grids.

An IoT-based EM system by adopting a cloud communication channel for networked devices in smart local areas was proposed [112]. This type of connectivity provides the data privacy, interoperability, redundancy, flexibility, and real-time features needed for EM. The proposed technology is based on global and local communication layers that rely on HTTP TCP/IP and MQTT protocols for cloud interactions. The communication infrastructure of the SG was analyzed, the protocols used in communications were verified, and the system's vulnerabilities to CAs were identified [82].

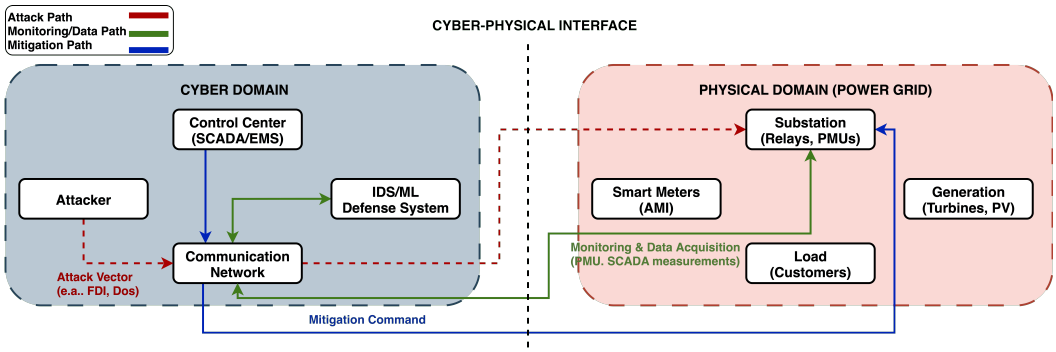

Figure 4. Smart Grid Cybersecurity: Cyber-Physical Attack & Defense Framework.

A secure communication protocol based on time, hash, and private vital constraints has also been proposed using the Sample Value protocol and the General Object Oriented Substation Events protocol. The proposed protocol creates a secure session key and then verifies it via authentication. The proposed protocol was implemented using the AVISPA tool, and its security was verified. A hybrid energy-efficient dynamic scheduling MAC protocol is proposed and is used for traffic-adaptive WSNs [113]. The proposed protocol consists of group or cluster formation and data transfer. In the cluster formation stage, the Variable Step Size Firefly Algorithm is proposed to generate energy-aware clusters by optimal selection of cluster heads. Its main function is to reduce the cost of determining the optimal placement of key nodes in the cluster. The following criteria: residual energy, node degree, number of possible group vertices, and distance within the group are considered criteria for selecting the objective function. Delay, latency, and overhead are reduced and controlled by data communication during the data transfer phase. The proposed approach has proven to help users reduce power consumption, extend network lifetime, and reduce overall overhead. A detailed SG Communications Network survey was presented [114]. The requirements of architecture, communications networks, applications, and technologies were studied.

A new scalable and flexible SGCN using cognitive radio (CR) technology is proposed. The proposed approach uses multiple layers through which the communication spectrum is divided into Wide Area Network, Neighborhood Area Network, and HAN. To facilitate the key agreement between the cloud server and the smart card/user via a TA, an improved and secure authentication scheme was proposed [83]. The proposed system was applied to the cloud server and SM. The proposed system is resistant to known attacks, which leads to a slight increase in communication and computation costs. Using formal analysis supported by a discussion of security features, the security of the proposed system is verified. The Robust Cramer Shoup (RCS) Delay Optimized Fully Homomorphic system was proposed for privacy-preserving and secure data transfer for deep learning (DL) [115]. The proposed approach is based on three steps: First, use the Kullback–Leibler divergence in the RCS decoding mechanism to reduce the communication burden and time. Second: The Delay Full Homomorphic Encryption mechanism is designed to reduce data access time and network delay. Third: To transfer data securely and preserve privacy, privacy-preserving DL using RCS Delay and Delay Optimized Fully Homomorphic Encryption is used.

A methodology is proposed to obtain accountability metrics in the cloud. The proposed methodology consists of three stages [116]. First, a conceptual analysis of these features is conducted to analyze the features of accountability into concrete mechanisms and practices. Second: Relevant control frameworks are analyzed to guide the implementation of security and privacy mechanisms related to the practices and mechanisms identified from the first step and used to identify measurable factors. The Cloud Control Matrix, privacy controls from NIST SP 800-53, and the Generally Accepted Privacy Principles were used for this

analysis. Third: Specific measures (either quantitative or qualitative) for these factors are extracted. To encrypt information and enhance the security of IoT communications while maintaining ease of use. An asymmetric ECC algorithm is proposed [117]. The role of ECC in lightweight authentication mechanisms is discussed in Section Authentication Methods and Privacy Protection. As for the process of storing information, compressed sensing has been proposed. Data compression is reconstructed using BCs to improve the speed of data storage in the IoT.

Using the Web of Objects and cloud architecture, an interoperable IoT platform for SHs is proposed [118]. The platform provides SH data in the cloud to benefit from SPs' applications and analytics. Through the platform, home appliances can be controlled from anywhere. First, to interoperate between different communication technologies and protocols and various old home devices, a gateway based on Raspberry PI was proposed. Second: Through the Representational State Transfer framework, SH devices are uploaded to the web and made available. Third: To store home data, a cloud server is provided for SHs, and data is provided and analyzed by various application SPs. A new hybrid communication approach based on Enterprise Service Buses (ESBs) was proposed [119]. This approach adds limited delay tolerance to strict real-time communication. This is done using additional fault-tolerant features that extend the core mechanism by adding failover behavior to the ESB-based connection. The proposed approach allows the system to continue running even when messages are violated and also allows fault isolation for timing violations to be available. Using Monte Carlo simulations, the introduced fault tolerance features are analyzed. With two direct methods for hard real-time communications, the throughput of the resulting data is compared. Attacks targeting different network layer functions in CR networks were classified [120]. Attacks found in traditional wireless networks were also analyzed, and their feasibility in CR network was studied. Based on the specifications of some attacks, it is detailed that they can only occur in the CR network, such as primary user activity and spectrum availability. Current mitigation techniques for each attack are also presented. Attention was paid to a wireless communication system with energy harvesting and error correction codes [121]. The optimization algorithm for transmission power, code rate, and modulation scheme is jointly studied. The goal is to maximize the actual average information transfer rate. The method for determining the Raptor code coding rate is first given within the known SN rates. The formula for the actual transmission rate is deduced using a specific coding and modulation rate. An optimization problem is created to maximize the actual average transmission rate. Using the Lyapunov optimization framework, the original long-run optimization problem is transformed into a single problem per time period. Through simulation, the proposed algorithm was verified.

A review of power line communications (PLC) for the SG was done [122]. The status, progress, challenges, and opportunities were discussed. PLC-based solutions/systems for renewable energy (RE) integration are reviewed in terms of Distributed PS and DERs monitoring/control and management modules. A detailed review of standards for the use of PLC in the field of SG has been carried out [123]. A study was also conducted on using PLC technologies in SG applications to determine the extent of PLC compatibility. To improve the problems related to PLC, the advantages and disadvantages of PLC for SG applications were analyzed. Proposed new standards and protocols for PLC were reviewed to standardize possible solutions. To reduce the processing time and network traffic while maintaining the privacy of each user, a data communication system for the AMI network was proposed [124]. The proposed system helps reduce the burden of encryption, as the assembly and encryption processes are carried out in a hybrid manner, which enhances the applicability of various SG applications. The results show that the proposed system has less coding overhead, especially when the number of SMs per capacitor is very large. A global

resilience measure has been demonstrated in the context of synchronous Communication Network (CN) [125]. The resilience measure expresses the system's ability to return to an operational state after a failure. An evaluation methodology for SC network plasticity has also been proposed. The ubiquitous sensor network of the International Telecommunication Union was studied and applied to the SG [126]. The technologies needed for secure and resilient communication using the ubiquitous sensor network's schematic layers are demonstrated. The weaknesses of the mentioned system and challenges were studied, as well as the pros and cons. Factors that can influence the choice of communication techniques are discussed. Possible communication technologies at different USN layers have been proposed. To address the problems of interoperability and scalability, the USN middleware system is discussed.

The comparative analysis of communication protocols in Table 3 is synthesized from the technical specifications, performance benchmarks, and vulnerability assessments reported in the reviewed literature on SG communications. The ratings for characteristics like latency, data rate, and susceptibility are relative comparisons based on typical operating conditions for each protocol. For instance, the high jamming susceptibility of ZigBee and Wi-Fi is a well-documented consequence of their operation in the crowded, unlicensed 2.4 GHz ISM band, while LoRaWAN's long range and low jamming susceptibility are due to its spread spectrum technique.

Table 3. Comparative analysis of communication protocols for Smart Grid networks.

Protocol	Typical Latency	Data Rate	Range	Susceptibility to Jamming/Interference	Primary SG Application
ZigBee	Low (ms)	250 kbps	Short (10–100 m)	High (2.4 GHz ISM band)	HAN (In-home display to meter)
Z-Wave	Low (ms)	100 kbps	Short (30 m)	High (900 MHz/2.4 GHz)	HAN
Wi-Fi	Very Low (ms)	100+ Mbps	Medium (50 m)	High (2.4/5 GHz ISM band)	HAN, limited NAN
LoRaWAN	High (s)	0.3–50 kbps	Long (5–15 km)	Low (spread spectrum)	NAN (Meter to concentrator)
NB-IoT	Medium (1–10 s)	200 kbps	Long (1–10 km)	Low (licensed spectrum)	NAN, WAN
PLC	Variable (ms)	500 kbps–1 Gbps	Medium (km)	Medium (vulnerable to grid noise)	HAN, NAN (over power lines)

The comparative analysis in Table 3 highlights critical trade-offs for SG deployments. For instance, while ZigBee and Wi-Fi offer low latency suitable for real-time HAN applications, their operation in crowded ISM bands makes them highly susceptible to jamming and interference, a significant security concern. In contrast, LoRaWAN and NB-IoT, designed for Wide Area Networks (WANs), offer long range and better resistance to jamming (especially NB-IoT on licensed spectrum) but incur higher latency, making them suitable for non-critical meter data collection rather than real-time control. PLC provides a unique alternative using existing infrastructure but is vulnerable to noise on the power lines, which can be intentionally created as a DoS attack. Therefore, protocol selection is a critical security decision: HAN protocols prioritize speed but require additional security layers against jamming, while WAN protocols prioritize range and reliability for data aggregation but are ill-suited for time-sensitive protection schemes.

6. Machine Learning in Cybersecurity

ML techniques, such as Support Vector Machine (SVMs), XGBoost SVMs, DTs, Long Short-Term Memory (LSTM), and others, are currently being used to enhance protection against CAs and detect intrusions in SGs [127], as shown in Figure 5. This section will examine the research papers and studies on this subject. Table 4 shows the ML techniques

for detecting CAs in the SG. Some of these works have been mentioned in other sections because they are relevant to the topic. For example, a comprehensive survey was conducted to demonstrate the various ML-based methods for detecting CAs on SNs [128].

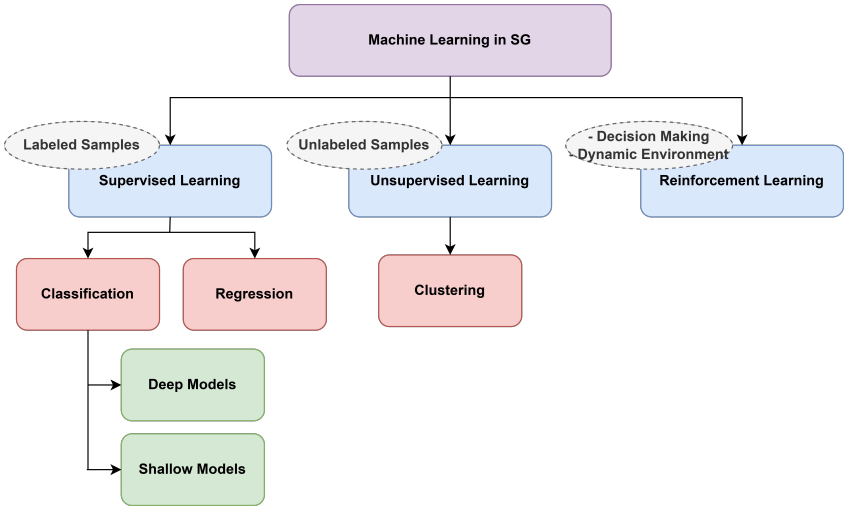

Figure 5. Machine Learning Techniques in Smart Grids.

A demand-side management (DSM) employs ML to protect the IoT from CAs [129]. DSM protects efficient energy use. A specific resilience factor model is proposed to manage SG's SG incursion and DSM. ML classifiers are used to predict fraudulent companies. A processing unit is introduced in the DSM engine to process energy data produced by the IoT-enabled HAN to optimize energy usage. The concepts of smart cities, their connection to SC, and how to employ them in this field were summarized and explained [130]. Many DL models were reviewed, such as Deep Belief Network (DBN), generative adversarial networks (GANs), Boltzmann machines, constrained Boltzmann machines, convolutional neural networks (CNN), and recurrent NNs. DBN processes data and transforms it into low-dimensional data while retaining essential features. For a security system with high accuracy and analytical ability, Recurrent Neural Network (RNN) is more suitable for classification than CNN. RNN-based functions, such as RNN-IDS, are essential factors in improving the accuracy of IDSs in SC [131]. While traditional Line-Commutated Converter (LCC) HVDC systems are generally regarded as having relatively low CS risk due to their simpler control structure and limited reliance on wide-area communication, the transition to multi-terminal LCC DC grids brings new vulnerabilities. These grids incorporate multiple inverter stations and require coordinated control over extensive communication networks—making them susceptible to cyber-physical attacks. Coordinated cyberattacks targeting multiple inverter nodes could disrupt stability or initiate cascading failures. Liu et al. [132] present grid-forming techniques and fault ride-through strategies based on fault current limiters in LCC-type DC grids, highlighting resilience at the control level. However, their work does not address CS attack surfaces or threat mitigation in such grid architectures. Thus, while these control strategies bolster operational robustness, further research is urgently needed to identify and defend against emerging cyber-attack vectors in high-capacity, multi-inverter DC infrastructures.

To effectively detect malicious attacks, a new interval state predictor is proposed [133]. The outer bounds of the state variables are formulated as a two-level optimization problem. Accordingly, any case outside the estimated limits can be considered an anomaly. To predict electrical loads, a DL algorithm has been applied that helps significantly improve prediction accuracy, called DBN. The effectiveness of the proposed system was verified on IEEE 14 and 118 bus systems. A new protection framework for cyber and physical systems of

SGs based on DL was proposed [134,135]. The proposed technique detects and addresses the CA using a set of techniques specifically designed for SG CS. Because SG CS datasets are asymmetric, this proposal creates new symmetric presentations for asymmetric risk management datasets. As in the proposed attack detection (AD) model, deep NNs and DT classifiers are used.

Table 4 provides a descriptive summary of the machine learning techniques discussed in the reviewed literature, mapping specific models to the types of attacks they were designed to detect and the datasets or systems used for validation. It is important to note that this table catalogs the reported applications and findings from the primary studies; it does not represent a direct, quantitative performance ranking of the models, as such a comparison would require a uniform benchmark across all studies, which is not available.

Table 4. Machine learning techniques for detecting cyberattacks in smart grid.

Ref.	Description	Attack	Model	Dataset/System
[126]	Protecting IoT from fraudulent companies	CAs	DSM	Realistic data from IoT-enabled HAN
[129]	Investigating the CS in SC	Not mentioned	DBN—GAN—CNN—RNN	Not mentioned
[130]	Anomaly-based detection using optimized interval state predictor	Malicious attacks	DBN	Realistic data from IEEE 14/18 bus system
[133]	Protecting cyber and physical systems of SG based on DL	CAs	Deep Neural Network (DNN)—DT	SG CS datasets
[134]	Reducing the computational cost by applying a small-scale ML model	Not mentioned	NAHL	EL-NAHL
[136]	Using IAI technique to classify anomalies	DoS—FDI	MSVM	Real-time digital simulator OPAL-RT
[137]	Detecting the FDI attack in SG using three independent methods	FDI	FDIDT—FDILR—FDILRT	Not mentioned
[138]	Investigating the efficiency of a multi-layer anti-attack defense framework	Typical passive attacks	Deep Autoencoder—Ensemble DNN	ns-3, FNCS and GridLAB-D simulators
[139]	Identifying the type of attacks in network communication channels	Physical layer attacks	Set of ML models	Simulated SG dataset
[140]	Investigating the CS in SCADA FOR ICS networks	malicious attacks	DBN—SVM	Not mentioned
[141]	Evaluating the performance of ML models in CAs detection	BOT-IoT	Set of ML models	Iot intrusion and anomaly identification dataset
[142]	Investigating the efficiency of SituRepair for critical infrastructure protection	mutation fault (MF)	Automated Program Repair (APR)	Code4Bench
[143]	Evaluating the performance of SML-DM model in SGCPN)	Cyber intrusions	SRS—DPE	Wireless sensor dataset
[144]	Utilizing IWP-CSO method to optimize HNA-NN in SCADA networks	Cyber intrusions	HNA-NN	Simulated SG dataset
[145]	Developing Smart Hybrid Technique (SHT) model to detect Deep Learning Algorithm (DIA) attacks in the hybrid MGs	DIA	SHT	HMG according to the IEEE standard system

A small-scale ML algorithm was proposed in SC to reduce computational costs [136]. The methodology is based on algorithmic complexity, imbalance, data complexity, and real threat scenarios. The proposed algorithm relies on an NN with an augmented hidden layer (NAHL) to accomplish learning quickly and efficiently. A label autoencoder (AE) approach is also introduced to solve the problem of data complexity concerning rapid

change and dynamism. The encryption approach is based on embedding labels into the NAHL structure (EL-NAHL) to take advantage of the spread of labels when separating sparse data.

An intelligent anomaly identification technique was proposed in distributed control-based cooperative MG AC systems [137]. Figure 6 shows data preprocessing and selection of learning types. The technology is based on data-driven AI tools, which use multi-class SVMs to classify anomalies such as Denial of Service (DoS) attacks, FDI attacks, etc. [146]. Optimal statistical features extracted from the measurements are used to train the Multi-class Support Vector Machine (MSVM). The proposed technique was validated on a real-time digital simulator OPAL Real-Time Technologies (OPAL-RT) by comparing it with Naive Bayes (NB) classification and Artificial Neural Network (ANN).

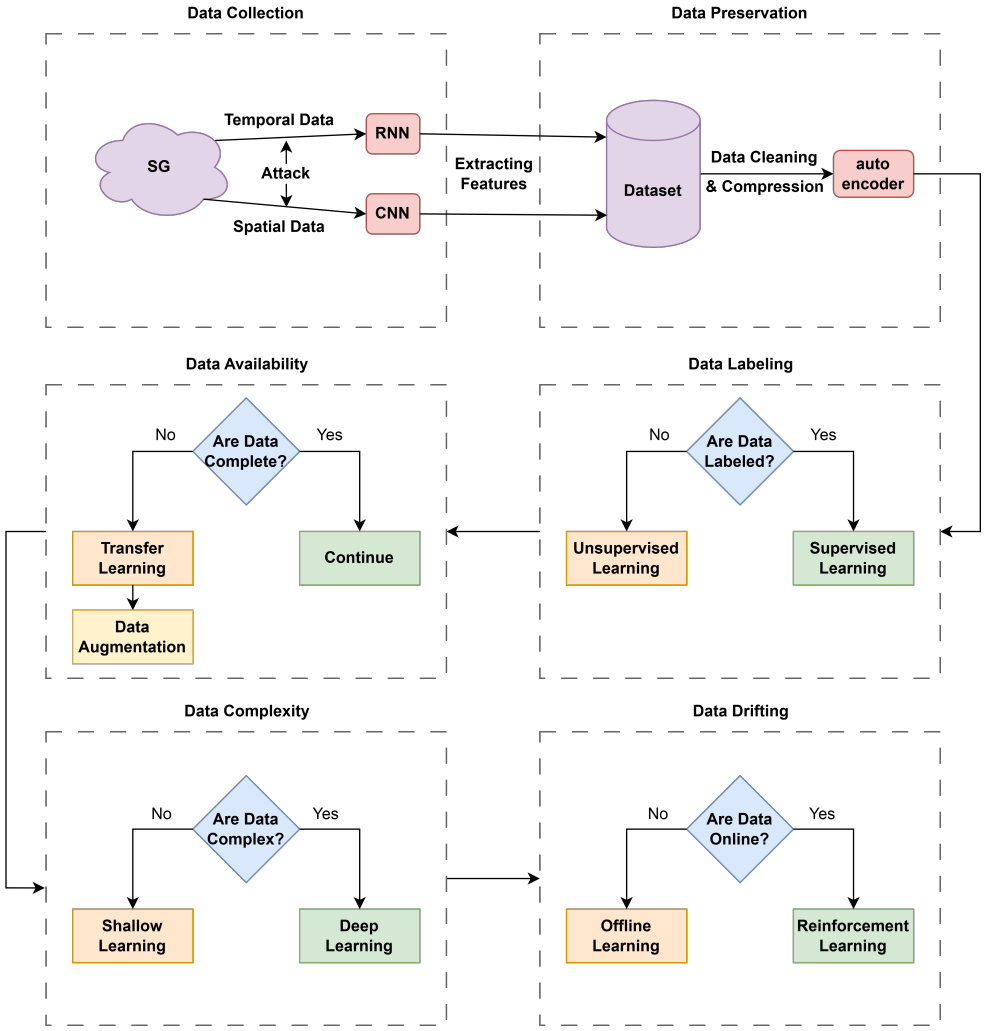

Figure 6. Data Preprocessing and Selection of Learning Types.

To confront the FDI attack in SGs, three independent techniques were proposed [138]. First: delta thresholding, linear regression, and linear regression with a timestamp. In addition, an algorithm is proposed to predict missing data. The strength of the proposed attack algorithms has been confirmed through the latest defense technologies.

Similarly, using different potential attack scenarios, a Q-Learning-based deep FDI attack generator was developed and configured with typical passive attacks [139]. Next, a multi-layer AD defense framework was created using the Deep Auto Encoder Network and Snapshot Ensemble Deep NN to detect known and unknown threats. The proposed model is verified using a combination of ns-3, FNCS, and GridLAB-D simulators.

An intelligent model for detecting and identifying attacks was proposed [140]. This model can classify the type of attack at the physical layer based on a set of machine-learning methods. In order to mitigate the impact of the attack on CNs, the proposed model converts the error or attack into specific measurements or features in the system. Unlike traditional ML algorithms, the proposed model adopts feature sorting based on hit probability. This sorting is verified by a chi-square test that ranks those features based on their association with each label. The proposed algorithm was tested on a SG dataset with 36 attack and fault scenarios simulated by Oak Ridge National Laboratories and using F1-Score and MCC classification.

A secure SCADA architecture was proposed for an ICSs network to protect the network from malicious attacks [141]. The proposed architecture is based on developing two detection model algorithms: a DBN and SVMs. The advantage of the proposed architecture is that it uses the payload feature and the network traffic feature for the detection model. DBNs detect attacks by forming Restricted Boltzmann Machines. For the SCADA network, batch methods for DBN have also been proposed. Different DBN structures are combined to create a set of DBNs for final detection.

A hybrid algorithm and framework model are proposed to solve the problem of choosing the effective ML algorithm among different algorithms to help the system detect CAs [142]. The proposed algorithm works by applying the IoT intrusion and anomaly identification dataset, and from several features of the ML algorithm, the 44 effective features are selected [147]. Figure 7 explains the methodology of AD in the SG. Then, five practical ML algorithms are selected to determine the most common ML algorithm performance evaluation metrics and identify attack traffic Bot-IoT. The binary soft ensemble approach and algorithm are applied to determine practical ML algorithms. An APR technique developed to repair Multiple Failure software was presented in [143]. Its purpose is critical infrastructure protection. The proposed model relies on ML to predict the type and status of error within the given program. The effectiveness of SituRepair has been verified through extensive experiments within Code4Bench.

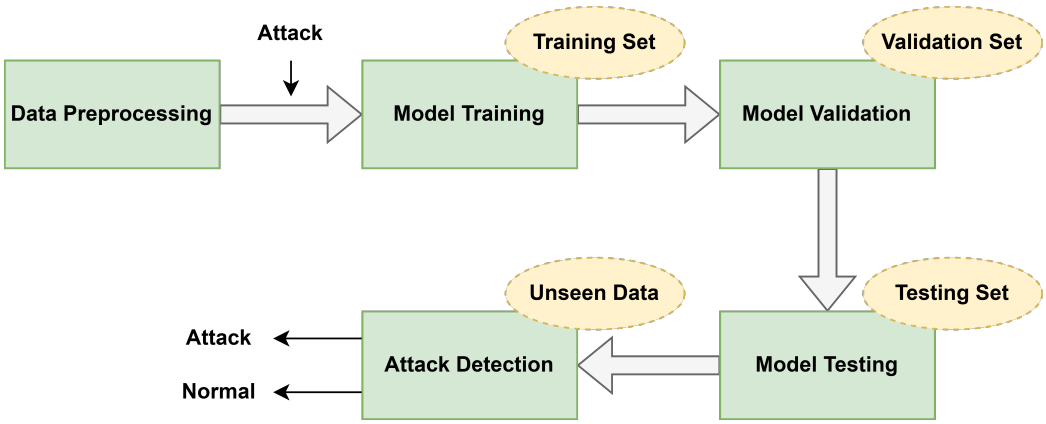

Figure 7. Methodology of Attack Detection in the SG.

A statistical ML defense mechanism is proposed to protect smart cyber-physical networks from cyber intrusion [144]. The proposed mechanism uses a mixture model of wireless sensor data with an embedded Gaussian. Two new indicators were proposed to evaluate the defense mechanism's performance. The first is the Sensor Reliability Score, which evaluates the reliability status of wireless sensors. Second, Data Prediction Error calculates actual and expected data errors during a CA.

Cuckoo search optimization techniques based on weighted particle and hierarchical neuron structure-based NN are proposed [145]. The proposed technique aims to detect and classify intrusions in a SCADA network to improve the network lifetime [148]. This

technique works by providing an input grid dataset as input, where selected features are arranged for further processing. Then, the features are improved using the proposed technique by reducing the dimensions of the features, which can effectively improve the accuracy. Finally, using the HNA-NN classification technique, the best-selected features are classified, which in turn classify intrusions into the network.

The impact of data integrity attack on the performance of hybrid MGs was studied [149]. A sequential hypothesis testing methodology has also been developed to detect these intrusions. The analysis statistic is calculated using a binary sample using the proposed approach. Then, a comparison is made with two thresholds to choose from among the three options. Real simulation work is performed in Hybrid Microgrid according to the IEEE standard system.

Despite their promising performance were showed, the deployment of DL models for cybersecurity in SGs faces several significant challenges. A primary concern is their data dependency; DL models require massive volumes of high-quality, labeled training data, which can be difficult and costly to obtain for rare but critical cyber-attack scenarios in operational grid environments.

Furthermore, the computational complexity of training and inferencing with deep networks (e.g., CNNs, LSTMs) may be prohibitive for resource-constrained edge devices like field sensors or relays, necessitating a cloud or fog computing architecture that introduces latency.

The black-box nature of many DL models also poses a critical problem for grid operators who require explainability to understand why an alarm was triggered and to take trustworthy corrective actions.

Finally, DL models are themselves vulnerable to adversarial attacks, where an attacker can craft subtle perturbations to input data that can fool the model into making incorrect classifications, thereby bypassing the detection system. These limitations necessitate a careful cost-benefit analysis and often lead to hybrid approaches that combine the pattern recognition power of DL with the transparency and reliability of traditional methods.

Table 5 gives critical comparison of which algorithms perform best under what circumstances.

Table 5. Synthesis of Machine Learning Algorithm Performance in Smart Grid Cybersecurity.

Algorithm Family	Strengths	Ideal Use Cases	Common Limitations
Tree-Based (RF, XGBoost)	High accuracy on tabular data, fast inference, interpretable	Intrusion Detection (network logs), Fraud Detection (energy theft), Classifying pre-defined attack types	Poor handling of raw sequential data, requires feature engineering
Deep Learning (LSTM/RNN)	Superior on sequential/temporal data, automatic feature learning	False Data Injection (FDI) attacks, Time-series anomaly detection, Load forecasting attacks	"Black-box", data-hungry, computationally intensive
Deep Learning (CNN)	Excellent spatial feature extraction	Malware detection (opcode sequences), Graph-based grid attacks	Less effective for pure time-series without spatial structure
Unsupervised (Autoencoders)	Works without labeled attack data, detects novel anomalies	Zero-day attack discovery, baseline modeling for system state	High false positive rate, difficult to classify attack type
Support Vector Machines (SVM)	Effective in high-dimensional spaces, robust to overfitting	Binary classification of attacks in feature-rich datasets	Poor scalability to large datasets, outperformed by newer models

7. Theoretical Frameworks for Defense and Attack

In this section, summaries of some scientific research and works that dealt with theories of defense or attack in the field of SC in SGs, particularly networks of other systems, such as the IoT, will be mentioned. Table 6 can Summarize the CAs in the SG. The Table 7 also Compares between shallow and DL for security objectives in the SG.

Table 6. Summarization of cyberattacks in the smart grid.

Attack	Description	Implications	Detection Models
Electricity Theft	Altering the electricity meter readings to reduce payments	Economic Losses—Damaging the SG infrastructure—Threatening the public safety	Fully-Connected Layer (FCL)—CNN—RNN—AE—DBN—GAN—Attention Mechanism (AM)
FDI	Compromising the system through injecting false data into the SG by malicious entity	Data misleading—Erroneous control—System instability	FCL—CNN—RNN—AE—ResNet—Graph Neural Network (GNN)—GAN—AM
False Command	Attacking the control center of the SG to generate unreliable data	Efficiency reduction—Increasing cost—Hazardous operational states	FCL—CNN—RNN—AE—DBN—GAN
Communication Traffic	Attacking the communication channels to decrease the integrity and availability of the SG	Delaying response time—Instability of system—Efficiency reduction—Damaging of equipment	FCL—CNN—RNN—ResNet
Adversarial Learning	Attacking the learning model by polluting training samples, modifying model's hyperparameters, or changing the input data	Disturbing the performance of learning model—Misleading output	FCL—CNN—RNN—AE—GAN—AM

Table 7. Comparison between shallow and deep learning for security objectives in SG.

Security Objective	Learning Type	Data Realisticity	Representation Learning	Adaptive Learning
Confidentiality	Shallow	No	No	Yes
	Deep	No	Yes	Yes
Integrity	Shallow	No	No	No
	Deep	No	Yes	Yes
Availability	Shallow	No	No	No
	Deep	Yes	Yes	Yes

Yingmeng Xiang and Lingfeng Wang worked on developing an optimal budget allocation strategy and theoretical interaction between attack and defense to prevent LR attacks, where attack and defense interactions were integrated into the two-level modeling of these attacks [150]. An optimal budget allocation strategy is developed to defend critical substations to minimize the expected load loss subject to the attacker's capability. Strategies for enhancing SC were studied using game theory-based methods for different attack scenarios. Using simulation on an IEEE test system, the proposed strategies are tested. A method for creating and solving a game theory model to address SC problems was presented [151]. The game theory approach can be applied to manufacturing to measure system reliability and analyze different defense policies to counter CAs. The proposed method offers a unique approach to determining the contents of the game payoff matrix. This approach is achieved by integrating sustainment, recovery from attacks, production losses, and defense strategies, three characteristics of manufacturing systems, into the cost

function that represents reality in manufacturing systems. The lower bound method was also used to calculate NE and universal utility.

A practical approach for power transmission planners has been developed to secure PGs from CAs [152]. The approach is based on proposing a three-level multi-objective methodology between the defender (the system planner), the rational attacker, and the operator. A commonly used reinforcement strategy for network protection is also proposed. A new type of resource has been introduced within the concept of deception, which is considered an effective tool to mislead the attacker in strategic planning. In the model based on shared perception, the defender's deception is mathematically modeled by releasing false information about the defender's plan. In the event of deception failure, the risk of damage is reduced by programming preventive objectives to prioritize a reinforcement strategy. The benefits of deception to the system are also shown, which is called situational value. With three-level mixed integer linear programming, the problems are formulated. The method of generating the constraint and column was solved. Simulations of the proposed approach have been performed on WSCC 9-bus and IEEE 118-bus systems.

A framework was proposed called "Decepti-SCADA" [153]. The proposed framework applies deception as a technique to improve the SC posture of a network. The proposed model uses decoys to obfuscate the network, making it difficult for the attacker to find the real components. The proposed framework has two parts: the publishing side is represented by Decepti-Box, and ELKSUR represents the monitoring side. A Decepti-Visual graphical user interface has also been created to facilitate the performance of security tasks using the Decepti-SCADA framework.

Relying on data for cyber-physical SG systems, a new method for evaluating the time delay (TD) of Wide Area Measurement System was proposed [154]. It is a random-based quantitative model that studies TD attacks. Using M/M/1 queuing theory and signal avoidance methods, the probability distribution function of multiple arrival times in the spatial sequence is depicted, considering the transmitted process of the data packet in the cyber layer. Sklar's and copula theorem combine distribution functions with multiple delays into a new quantitative model of delay. According to the reason for generating the TD, it is divided into two parts: first, delay resulting from network attacks, and second, delay inherent. The delay caused by the first section is detected using the connectivity principle and likelihood ratio. The simulation was done on an IEEE 39 bus system. Application and case studies were performed on a ten-machine PS in New England. A solution to the FDIA problem was reviewed [155,156]. An efficient implementation methodology for identifying precise intrusion points in real-time based on DL was proposed [157]. Traditional bad data detectors work with DL models to identify FDIs within a measurement set [158]. The methodology uses multi-layer perceptual models, CNN, CNN-LSTM, CNN-BiLSTM, and a DT. The DL models used in the proposed methodology also capture inconsistency with simultaneous dependency on potential attack vectors. Network operators can also detect attacks in real-time without any initial statistical assumptions of the network through these models. The simulation was done on a standard IEEE test. A vulnerability indicator was proposed to counter FDIA [159]. The proposal works to secure the meters most at risk. The attacker works to corrupt the output of the state estimator by normalizing the meter readings. The proposed methodology is based on identifying a set of attack vectors called important attack vectors [160]. All attack vectors with lower costs will be avoided if important attack vectors with lower costs are avoided. The proposed methodology can classify counters based on the number of attack vectors attacking a device using significant attack vectors. An algorithm has also been proposed to determine which counters to secure. The proposed index was simulated using the IEEE test system. An algorithm was proposed to detect the moment when an attack on a CPS begins [161]. The algorithm is based on

the principle of retrospective research, not real-time. Via the back-end and back-of-the-observer approach, a batch-type detection algorithm for the attack moment is proposed. The proposed algorithm addresses the problem of "temporarily hidden" sensing attacks for polynomial types. These are types of attacks that traditional anomaly detectors can hardly detect the moment of attack in real-time.

A resilience-based grid recovery scheme is proposed to restore the SG after successful CAs on substations [162]. The proposed scheme is based on a measure developed to capture: First: energy-side resilience (PsR). This includes available spare capacity, load, reliability, and available line capacity, and these four characteristics are used to evaluate the resilience status of the SG through the proposed recovery measure (CPARM). Second: Cyber flexibility (CsR). The one that calculates the resilience of the physical side based on immediate damage is PsR. CsR calculates the resilience of the cyber side based on the potential damage to the system. Various SG constraints and capabilities such as automatic generator control (AGC) capability, transient stability, ramp rate, multi-stage attacks, and load changes during the recovery phase are incorporated to achieve a more realistic model. The proposed methodology has been applied to a 39-bus New England test system and a 30-bus IEEE test case.

Analysis and design of security of networked control systems based on an attack space based on the corresponding adversary model description, adversary model knowledge, disruption resources, and disclosure was proposed [163]. The proposed methodology analyzed various CAs, such as replay attacks, DoS attacks, bias injection attacks, and zero dynamics. Using the concept of secure clusters, the attack impact of each scenario is characterized, and the attack policy is described. A defense strategy was developed that considers distributed generators to increase the PG's reliability against coordinated attacks [164,165]. A robust three-level optimization model was developed to enhance defense strategies against cyber-attacks in SGs [166]. The lower level simulates the defender's response, optimizing energy flow and the placement of grid monitors. The middle level models the attacker's decision-making process. The top level determines the optimal pre-attack defense configuration, incorporating previously placed grid monitors. The model aims to reduce system load and improve resilience. It is solved using the Nested Columns and Constraints algorithm and tested on IEEE 14-bus and IEEE RTS79 systems.

The proposed model is based on determining the optimal defense strategy and formulating a coordinated attack scenario. The three-level optimization model consists of the following: First, the lowest level problem, in which the operator's actions to retransmit the system are carried out to reduce the unserved energy. Second, the attacker's behaviors are modeled in a mid-level problem that determines the attack time and sets goals to maximize unserved energy. Third: The planner's actions are formulated, and the optimal allocation of defense resources on the CN of protection relays determines the defense resources on transmission lines in the upper-level problem. The simulation was done on an IEEE 14-bus and IEEE 57-bus systems.

Additionally, a comprehensive security assessment was conducted on two critical data collection technologies in SGs: Phase Data Concentrators and Phasor Measurement Units (PMUs) [167]. These devices are crucial for the accuracy of SCADA and EM systems. The study highlights vulnerabilities such as weak password policies, unencrypted communication channels, and lack of input validation. To identify sparse attack vectors and determine the minimum sets of compromised measurements, the authors proposed an exact and relaxed integral reformulation to minimize cardinality [168]. What made it easier to solve the fundamental problem in the selected case was to express the integration constraints as a combination of linear constraints and SOS1 constraints. Vulnerabilities were examined and analyzed based on the Cartesian formulation in the presence of zero injection buses. FDI

Attacks were checked against the PMU linear state estimator. Simulations were performed on IEEE 14, 30, 57, and 118-bus standard systems. To accurately model LRAs resulting from FDIs, a mixed-integer linear programming model was developed to model these stealthy CAs [169]. The proposed model shows that attackers can only target an area of the PS and cannot access the entire SG system. The simulation was done on IEEE 118-bus systems. A two-level optimization model based on distribution network reconfiguration against FDIAs is proposed to mitigate the harmful effects of attacks and find the most vulnerable and effective attacks and the optimal response to ISOs [170]. First, To maximize the energy loss, the attacker launches his attack at the optimal location of the SMs, taking into account the pre-defined constraints, and this is at the upper level of the model. Second: As an ideal defense strategy to reduce energy loss, reconfiguration of the distribution network is proposed, and its effectiveness is verified, all representing the lowest level of the optimization model. The simulation was performed on a modified IEEE 94-bus system.

Using graph network (GN), a graph detection technique was developed to detect measurements tampered with due to CAs [171]. The capsule network was also developed along with GN. It detects the location of FDI attacks in any dimension of diverse energy systems. The proposed approach obtains detailed characteristics about each observation, such as direction, connectivity, location, etc. Simulation is done using IEEE 30-bus and IEEE 118-bus standard systems. Using the Markov decision process model, a framework was created to model the interaction between the dynamic CA process and specific response actions [172]. Its purpose is to enable the MDP agent to determine optimal response actions at NPPs. The optimal response is based on preventing the electronic attack from reaching a state of security failure and implementing FRP procedures, which in turn bring the station to a truly secure state despite the attack. The proposed approach modifies the existing action-value function, adopting a heuristic Monte Carlo Tree Search algorithm. The integrated response process to CAs in NPPs was analyzed [173]. A knowledge-based hidden Markov modeling method is developed to develop a security state estimation model [174]. To obtain improved estimation results in the developed security state estimation method, the generated HMMs can be updated online. This method helps operators perform cause analysis and security impact analysis. The developed method can be applied to measure the functional impact of the estimated current security state through integration with the PSA method. The Kalman filter algorithm was used to securely monitor the operating conditions of hardware components and keep them away from CAs. The application was made to the Hardware-in-the-Loop system, a part developed in an IAEA Coordinated Research Project. A distributed watermarking strategy is proposed to validate the information transmitted between the distributed generation units of DCmG and support the monitoring system used [175]. Its goal is to overcome replay attacks in networks. Through a hierarchical control structure, distributed generation units are organized. To ensure the detection of replay attacks, conditions were provided on the watermark, and such a signal was designed. Simulations are presented to demonstrate the effectiveness of this technique.

In response to the evolving sophistication of FDIAs, detection paradigms have shifted towards methods that leverage the underlying physics of the power grid, as summarized in Table 8.

These physics-aware methods provide a crucial layer of defense because they are designed to detect manipulations that violate fundamental physical truths, which are immutable and cannot be fooled by statistically clever false data.

It was proposed that an interactive dynamic game based on defense and attack be designed to control the PS's frequency [176]. The fundamental frequency control system proposes two types of stochastic game scenarios representing two collisional relationships between attackers and defenders. Among the possibilities based on SCG, first, when the

defense resource is sufficient, the defenders can stabilize the frequency until the attackers are the ones who adjust their actions. Second, When the defense resource is insufficient, the defenders cannot reach a balancing strategy. In LCG-based probabilities, Defenders can negotiate with attackers to achieve their optimization. Improved defense strategies based on NE were studied using reinforcement learning algorithms.

In another research, a model was proposed to develop algorithms to detect foreign investment attacks that threaten SNs and work to mitigate their damage [177]. A set of critical concepts that cause significant deviation in the data distribution from the basic concept is proposed instead of using only historical data for the basic concept. Using the PCA and KS tests, this group was calculated. The k-NN algorithm was used to verify the results. The model was evaluated on an IEEE 14 bus system according to two different attack scenarios: the first is attacks under concept drift. Second: Attacks without concept drift.

Table 8. A Taxonomy for Smart Grid Cyber Threat Prioritization.

Stealthy FDIA Variant	Description & Goal	Physics-Aware Detection Mechanism	Key Principle
Ramping (Slow-Drift) Attack	Injects false data gradually to slowly bias state estimation over time. Evades traditional BDD by mimicking legitimate load ramping.	Dynamic State Estimation (DSE)	Uses a model of system dynamics (e.g., generator swing equations) to predict the state. Flags inconsistencies between the physics-based prediction and measured values, catching slow drifts.
Topology-Aware Attack	Attacker compromises knowledge of grid topology (e.g., line outages) to make false data consistent with the current network model.	Kirchhoff's Law Validation	Continuously checks measurements for adherence to fundamental physical laws (e.g., power conservation at a node). Flags any violation as an anomaly, regardless of statistical residual.
Data-Driven FDIA (e.g., using GANs)	Uses machine learning (e.g., Generative Adversarial Networks) to create false measurements that replicate the statistical properties of real noise and load patterns.	Physics-Informed Neural Networks (PINNs)	Integrates physical law constraints (e.g., power flow equations) directly as a penalty term in the neural network's loss function. Makes the model learn from both data and physics, improving robustness to mathematically plausible but physically impossible data.

Several ML algorithms such as random forest, DT, and gradient boosting machine (GBM) were tested on an IoT dataset [178]. By comparing the algorithms, it was concluded that the DT algorithm is the most accurate and has better AUC scores than other ML methods. The algorithms were analyzed using different analytical methods such as naïve Bayes and linear and quadratic discriminant analysis. The random forest algorithm is better at AUC because it combines the results of multiple individual DTs. As for the GBM algorithm, it works well, but it is poor in terms of accuracy and time.

As a malicious DA, an analytical methodology for the cyber-physical security of SG is presented [179]. The methodology is based on the following steps: Proving how parameter errors spread in the measurement function. Second, The most significant characteristic of the composite normal measurement error (CMEN) is identified. Third: A methodology is presented to correct malicious data injection in the SG. Using the Critical Fault Analysis measurement framework, attacks are processed simultaneously and analyzed [180]. Through Chi-square (χ^2) HT applied to CMEN, the CA is detected. Using the Measurement Innovation Index, synthetic errors are estimated. The proposed methodology has been verified using IEEE 14-bus and 57-bus systems.

An edge-based federated learning framework is proposed to detect FDI attacks on PG state estimation [181–183]. An incentive mechanism encourages data owners to contribute to AD to obtain high detection accuracy with limited measurement datasets. A new preference criterion is proposed to achieve optimal detection accuracy. A two-level model depicting the involvement of data subjects in AD is formulated to explore the impact of the incentive mechanism on detection accuracy, which is then quantitatively measured. The incentive mechanism was designed and tested for 100 Monte Carlo scenarios.

A set of concepts and methods from systems disciplines were applied to CAs in SGs [184]. Systems engineering has been applied to cyber-physical security problems. Parts are designed and standardized based on fault-tolerant design and concepts from systems engineering.

While studying cyber-physical security, a nonlinear AGC model was designed [185]. Potential weaknesses that may result from ignoring nonlinearities are analyzed. The impact of FDI and TD attacks against AGC systems has been studied. A DL approach is proposed based on an LSTM algorithm to address potential threats [186]. The proposed algorithm detects anomalies in the data resulting from TD and FDI attacks. Then, it reduces the compromised signals to reduce the impact of these attacks on the system. The proposed model was measured and evaluated using a two-zone AGC system.

It was demonstrated that an undetectable attack could be carried out despite only knowing a specific section of the PS [187]. The attack and its implementation are demonstrated using the Bad Data Detection algorithm on a widely adopted IEEE 14 bus system. To protect against CAs, a method is proposed to select a subset of available measurements.

The design problem of flexible load frequency control of a multi-zone PS with uncertainty and physical constraints under DoS attacks and transmission delay is investigated [188,189]. The switching and TD systems were used in elastic analysis to derive the stability criterion. To maintain the exponential performance of H00, sufficient conditions have been derived. The government's feedback control law is designed to allow DoS attacks.

Using Software Defined Networking (SDN), a systematic review of CT categories and defense methods was conducted [190,191]. It is a technology that improves the way security is achieved due to its cost-effectiveness, flexibility, and suitability for incremental deployment. To prevent or mitigate classified attacks, SDN-based solutions have been classified as attacks: spoofing, scanning, sniffing, DoS, malware, web application attacks, and social engineering.

In content similar to previous works, an analytical methodology for cyber-physical security in SGs is presented [192]. The proposed methodology analyzes critical errors and can detect and correct malicious attacks in SNs. The principle of the proposed methodology is based on classical WLS state estimation based on the state estimator formula. Through the chi-square (χ^2) hypothesis test applied to the CMEN, the CA is detected. With the Measurement Innovation Index, synthetic errors are estimated. Through the largest error testing feature, the identity of the CA is determined [193]. The proposed methodology was verified on IEEE 14-bus and 57-bus systems.

A correction model for CAs on SGs that inject false data is presented [194]. The methodology uses a Taylor series approximation matrix and correction of the Jacobian parameters (τ). A framework for measuring critical error analysis has been published in the treatment and analysis of CAs. The CMEN, the Chi-square (χ^2) hypothesis test, is applied to detect CAs. For identification, the CMEN maximum error test is used. The proposed methodology has been verified on IEEE 14-bus and 118-bus systems.

An SC defense framework is proposed to enhance the stable operation of the Fast Frequency Reserve control system based on the Wide Area Monitoring System [195]. The

proposed framework is based on time-frequency dependence and is called CWTs-DSCNN to detect cyber spoofing of synchronous phase data. This approach works in two steps: First, continuous wavelet transforms are needed to analyze the impersonation signals. Second, Dual-frequency scale CNNs were proposed to determine the matrix of time-frequency fields. Multiple experiments were conducted using actual data from FNET/GridEye to verify the effectiveness of the proposed framework.

The comparison in Table 9 reveals inherent trade-offs that dictate solution selection for different Smart Grid applications: For Resource-Constrained Edge Devices (e.g., Smart Meters, Sensors): Solutions with low computational overhead and cost are paramount. Here, PUF-based authentication presents a compelling advantage over traditional PKI, as it eliminates the need for complex key management and secure storage in inexpensive devices. However, its lower maturity requires careful consideration. For Core Network and Control Center Defense: Attack coverage and resilience are the highest priorities. ML-based IDS excels here, providing broad coverage against a range of attacks like FDI and DDoS by learning normal network behavior. Its weakness to adversarial attacks can be mitigated by combining it with other methods. For High-Value, Auditable Transactions (e.g., V2G payments): Trust and non-repudiation are critical. BC offers a unique value proposition with its tamper-proof ledger, ensuring the integrity of financial and energy transactions. However, its prohibitive cost and latency make it unsuitable for real-time control functions. For Strategic Resource Allocation: Game-theoretic models are powerful tools for a system operator to preemptively allocate limited defense resources (e.g., where to place intrusion detectors) based on potential attacker incentives. Their value is strategic rather than tactical, and they are best used for planning rather than real-time operation. This analysis underscores that there is no "silver bullet" solution. A defense-in-depth strategy is essential, where a combination of these solutions is deployed in a layered architecture. For example, PUF could secure device identity at the edge, ML-IDS could monitor network traffic for anomalies, and BC could log critical operations at the control center, each playing to its respective strengths while compensating for the others' weaknesses.

Table 9. Comparative Analysis of Primary Cybersecurity Solutions for Smart Grids.

Solution Category	Deployment Cost & Overhead	Attack Coverage Strength	Attack Coverage Weakness	Implementation Maturity
Public Key Infrastructure (PKI)	High (CA setup, key management)	Strong authentication, non-repudiation, integrity	Vulnerable to quantum attacks, complex for large-scale IoT	High (Well-established standard)
Physical Unclonable Functions (PUF)	Low (Hardware-based, no key storage)	Resilient to physical tampering, clone-resistant	Requires secure enrollment, challenge-response latency	Medium (Emerging, research testbeds)
Machine Learning (ML) for IDS	Medium (Data collection, model training)	Excellent for detecting novel FDI, pattern recognition	Vulnerable to adversarial examples, data quality dependent	Medium-High (Commercial products exist)
Blockchain	Very High (Consensus computation, storage)	Tamper-proof logging, decentralized trust, transparency	High latency, low throughput, significant energy cost	Low (Mostly pilots and prototypes)
Game Theory	Medium (Model design, computation)	Proactive defense, strategic resource allocation	Relies on accurate attacker models, computational complexity	Low (Theoretical/Simulation mostly)

8. General Applications of Cybersecurity

This section mentions that some general applications of SC in SNs and other sectors such as trading, e-commerce, the self-driving car sector, and others. And also Table 10 Summarize some vital applications in the SG.

Table 10. Summarization of some vital applications in the SG.

Reference	Application	Method(s) Used
[195]	Distribution Management	Time-frequency dependence using Continuous Wavelet Transform and Dual-Scale CNN (CWTs-DSCNN), validated on FNET/GridEye data
[196]	SCADA	Interface Damping Impedance Method (DIM) for MMC-HVDC PHIL simulation, using trapezoidal integration
[197]	Outrage Management	Inverse Stackelberg game theory; multilevel sub-games; closed-form NE strategies; IEEE 2030.5 standard
[198]	Outrage Management	Reinforcement learning-based adaptive protection with environment-agent interaction and reward design
[199]	Advanced Metering Infrastructure	Security requirement-to-control mapping model; includes 7 security requirements, 9 threats, 45 security controls
[200]	Advanced Metering Infrastructure	Power System Energy Structure (PSES); DLF; low-frequency oscillation analysis
[201]	Asset Management	Noise addition technique using random values to protect privacy in SM communication
[202]	Demand Response Management	Coordinated cyber-physical attack (2-stage); AC state estimation; contract price manipulation; IEEE 14, 39, 118-bus systems
[203]	Distribution Management	Whale Optimization Algorithm; BC-based architecture; copula model for layout randomness
[204]	Outrage Management	ResNet-ALSTM deep learning model; FDIA detection and recovery; regression & multi-label classification; IEEE and Belgian test systems
[205]	SCADA	LMTracker algorithm using heterogeneous graph, unsupervised anomaly detection, and traffic/event logs
[206]	Asset Management	Real-time CPS with SEL 351S and OPAL-RT; optimized offline power flow via PowerWorld
[207]	Advanced Metering Infrastructure	Theoretical analysis of BC for RE and Security
[208]	Electrical Vehicles Charging	Robust hybrid state estimation algorithm; modified WLS using PMU and SCADA measurements
[209]	SCADA	Fault-tolerant/threat-tolerant platooning system; includes AGV communication with fog/cloud and assurance case analysis
[84]	Demand Response Management	Bellman-Ford-based path calculation; AI-based data routing; hierarchical certificate management for IoT
[210]	Asset Management	Managed Industrial Security Services (MISS); role in system stability and ESG impacts
[211]	Outrage Management	Meta-simulator architecture for SG applications; supports IoT protocols and cross-framework synchronization

Guoqing Li et al., 2018 an improved interface damping impedance method algorithm is proposed for the MMC-HVDC PHIL simulation system to deal with the stability and accuracy problems caused by the power interface [196]. To simplify the calculation of the equivalent impedance of the MMC, the turn-off resistance of the power device is set to infinity. The trapezoidal integration method is used to differentiate the subunit amplitude. In this way, effective impedance matching of the DIM is achieved.

A decision support system was developed to determine the equitable allocation of financial resources for implementing a distributed energy resource management system [197]. A multilevel structure of interconnected sub-games is mapped through utility functions using the inverse Stackelberg game theoretic approach. Optimal energy brokerage is verified mathematically, with the existence and uniqueness of an NE, and by providing closed solutions for NE strategies. Through a non-iterative algorithm, the dependence of NE on very general inputs and parameters is demonstrated, verified, and implemented via the IEEE 2030.5 standard system.

To solve the problem of protection coordination from the perspective of sequential decision-making, an environment-adapted protection plan is proposed [198]. To enable the protection agent to adapt, the interaction between the agent and the environment is designed to incorporate protection-related knowledge. The protection plan is based on preventive sequences based on reinforcement education. Reinforcement learning relies on three main elements: in the field of protection, identifying invalid and direct actions, systematically embedding states in the value table to reflect the response time of the relay, and carefully designing the reward. The proposed system is simulated with a 14-bus and 38-bus system.

In the two-way data flow of the SG, a model was developed that bridges the gap between requirements and controls for SC [199]. The proposed model contains seven security requirements, seven access points, nine threats, and 45 security controls to counter CTs and attacks.

An online tracking method was proposed for the damping contribution of a multi-machine PS and the dominant oscillation paths [200]. The proposed method is based on two optimized forms of the PS energy structure and the damping loss factor (DLF). To quantitatively determine the relationship between dissipation energy and damping ratio for each case, DLF is introduced in elastic mechanics. The composition of the dissipation energy during low-frequency oscillation is analyzed based on the PSES framework. Two improved forms of PSES with different dissipation energy distributions are derived based on the dominance of the aperiodic component in the dissipation energy. The simulation was done on China's 16 machines, five zones system as a practical PS.

A lightweight method was proposed to address how to protect consumers' privacy when using SM systems using noise addition [201]. The proposed system generates a random number in the communication between the SM and the power supply. It adds this number to the measurement to be sent to the power supply.

A coordinated cyber-physical attack based on AC State Estimation was proposed to disrupt the market by manipulating the contract price [202,212]. The proposed attack consists of two stages. The first is identifying the weakest branch in the network, which causes the maximum deviation in the contract price allocation between the pre-attack and post-attack scenarios. Second, An electronic attack is manufactured to hide the effect of a physical attack. The proposed model was verified using IEEE 14.39 and 118 Bus PSs.

To find an optimal solution for system-level EM, the Whale Optimization Algorithm was developed [203]. To increase the security of DC/AC power trading and data exchange architecture in hybrid MGs, BC technology has been applied. According to the copula model, random convection flow was used to create a realistic layout.

For rapid economic distribution in PSs of Electricity and Gas CPSs with FDI Attacks, a new approach called ResNet-ALSTM based on cyber-physical data is proposed [204]. The proposed approach links the attention LSTM model with the residual network (ResNet). This approach employs a multi-label classification and regression model to solve the FDIA location detection problem. A Fast Dynamic Time Warping algorithm has been implemented to restore tampered measurements in time upon FDIA detection. A regression model is applied to achieve rapid economic distribution in Electricity and Gas Cyber-Physical System (EGCPS). Case studies were done on a 24-bus IEEE PS and a 20-node Belgian gas system.

Based on the heterogeneous graph to detect the attack path, the LMTracker algorithm was proposed [205]. The proposed algorithm consists of three modules: path representation generation, heterogeneous graph construction, and unsupervised anomaly-based attack path detection. The proposed approach uses event and traffic logs to implement anomaly-

based path detection. This is done by creating vector representations of lateral motion paths, generating heterogeneous graphs, and using an unsupervised algorithm.

A real-time CPS is proposed for stability control and attack simulation [206,213]. The SEL 351S protection system was used with OPAL-RT. Using the PowerWorld simulator, an optimized off-line power flow was implemented to prevent the system from becoming unstable. A comprehensive theoretical study of BC and its importance in RE was conducted [207]. The importance of this technology in the field of RE and SC is noted. To address the presence of bounded data uncertainties, a robust hybrid state estimation algorithm was proposed [208]. The proposed algorithm works through PMUs and SCADA measurements. The formulation of the WLS method was modified to eliminate the effect of uncertainty in both measurements and network parameters [214]. The simulation was performed on an IEEE 30-bus system.

A comprehensive approach to fault-tolerant and threat-tolerant platooning was proposed for material transportation in production environments [209]. The proposed approach includes a set of functional instances, including communication with fog and cloud levels, data acquisition and processing by range consideration, and platoon control for collision avoidance. Using platooning of automated guided vehicles (AGVs), assurance cases are created to demonstrate safety using Hazard and Operability and Threat and Operability techniques.

An approach using reliable sensing techniques was proposed to provide reliable remote sensing and collection for future generation systems [84]. The proposed model uses the Bellman-Ford method, and weighted calculation evaluates the available paths. The proposed approach works in stages: First, Search between IoT devices and mobile stations to transfer data using a method based on AI. Second: Supporting digital certificates for MA by establishing a solid security method between one peer and another. Third: Sending the certificates in the form of a series to maintain their integrity. Fourth, Trust and privacy are used to store data on cloud servers.

In [210], they focused on managed industrial security services and discussed their role in the industrial system's stability and its impact on the environmental, economic, and social system. In other work, a meta-simulator architecture capable of simulating any electrical PS application was proposed [211]. The proposed device only needs to define a set of behavior rules. The proposed device reduces the amount of knowledge needed to deploy new applications. The advantages of the proposed architecture are that it is compatible with IoT protocols, lightweight, intelligent systems, and supports synchronization with other frameworks at different levels. On wind farms, gaps in understanding the threats to which they are exposed and their impacts have been highlighted [215]. The components of a wind farm and the attack vectors through which IT, industrial control, and physical assets are targeted are described.

9. Discussion and Limitations

9.1. Synthesis of Key Insights

This comprehensive review has illuminated several dominant trends and critical insights in the field of Smart Grid and IoT cybersecurity. The integration of Machine Learning and AI, particularly Deep Learning, is now a central research theme, demonstrating remarkable success in detecting complex and stealthy attacks like False Data Injection. However, our analysis consistently reveals a significant gap between theoretical proposals and practical deployment, often due to the "black-box" nature of these models and their substantial computational demands.

Furthermore, the review highlights the critical importance of a holistic defense-in-depth strategy. No single technology is a silver bullet. The most resilient future SG will

likely leverage a combination of lightweight cryptography for edge devices, robust communication protocols for data-in-transit, AI-based monitoring for anomaly detection, and theoretical frameworks like game theory for strategic resource planning. The convergence of the SG with other domains, such as e-commerce and autonomous systems, is not just a source of new threats but also a valuable source of innovative security solutions, such as blockchain for tamper-proof logging and control-theoretic approaches for assured resilience.

9.2. Limitations of the Review

While this review aimed to be as comprehensive as possible, it is subject to several inherent limitations that should be acknowledged.

First and foremost, the scope and findings of any literature review are intrinsically shaped by the search strategy. While our Boolean search string was designed to be broad, it is possible that relevant studies using different terminology were inadvertently missed. The review's focus is also constrained by the selection of academic databases (Scopus, Web of Science, IEEE Xplore). Although these are leading indexes, they may not capture all relevant industry whitepapers, technical reports, or publications in non-indexed journals.

second, a significant challenge in synthesizing this field is the lack of standardized benchmarks and evaluation metrics. The studies reviewed here use a wide variety of datasets (often synthetic or from different testbeds) and performance metrics, making a direct, quantitative comparison of the reported efficacy of different solutions extremely difficult. This limitation underscores the community's need for open, standardized SG cybersecurity datasets.

Finally, the rapidly evolving nature of both cyber threats and defensive technologies means that this review represents a snapshot in time. New attack vectors and cutting-edge solutions, particularly involving generative AI and quantum computing, are emerging at a pace that is challenging for any comprehensive review to fully capture. These limitations, however, also point toward valuable opportunities for future work.

10. Conclusions

This article reviews and summarizes the latest developments in CS in SG and IoT environments. The paper highlights the key technologies used and the security risks they face. The reviewed research also focuses on authentication mechanisms, privacy protection, communication protocols, and ML-based CS.

This paper provides researchers with a summary that helps them explore the many different technologies in CS and their applications in SGs and the IoT. If researchers are interested in these areas, particularly in terms of communications in these systems and the threats they face, they will find the most prominent research addressing this issue in the Communication Protocols Section. If researchers wish to research machine learning systems in these systems and their role in addressing CS challenges, they will find a dedicated section in this paper, and so on. This facilitates access to shared information from multiple research papers.

In the second section, a current authentication and privacy-preserving techniques are presented, focusing on simple cryptographic systems such as ECC and PUF, which are critical for resource-constrained devices. The third section detailed communication protocols relevant to SGs, including ZigBee, LoRaWAN, and MQTT, and discussed the trade-offs between their security and efficiency. The fourth section focused on machine learning applications in intrusion detection and anomaly detection, emphasizing the importance of real-time and federated learning frameworks. The fifth section addressed theoretical frameworks for defense and offense against cyberattacks, such as game the-

ory and deception-based defenses (e.g., Decepti-SCADA), highlighting their potential for proactive threat mitigation.

Future Research Directions: To advance this field, future research should examine the scalability of deception-based frameworks in operational SG environments, evaluate the performance of post-quantum cryptographic systems, and establish unified standards for machine learning-based IDSs. In addition, federated learning and zero-trust frameworks represent promising models for distributed CS in SG.

Funding: This research received no external funding.

Acknowledgments: The authors would like to convey their most heartfelt appreciation of this review article.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

AA	Anonymous Authentication
AD	Attack Detection
AE	Autoencoder
AGC	Automatic Generation Control
AGV	Automated Guided Vehicle
AI	Artificial Intelligence
AM	Attention Mechanism
AMI	Advanced Measurement Infrastructure
ANN	Artificial Neural Network
BC	BlockChain
CAs	Cyber Attacks
CC	Cloud Computing
CMEN	Composite Normal Measurement Error
CN	Communication Network
CNN	Convolutional Neural Network
CPPS	Cyber Physical Power System
CPS	Cyber-Physical System
CR	Cognitive Radio
CS	CyberSecurity
CTs	Cyber Threats
DA	Data Attack
DAE	Deep Autoencoder
DBN	Deep Belief Network
DER	Distributed Energy Resources
DL	Deep Learning
DLF	Damping Loss Factor
DNN	Deep Neural Network
DoS	Denial of Service
DSM	Demand-Side Management
DT	Decision Tree
ECC	Elliptic Curve Cryptography
EM	Energy Management
ESB	Enterprise Service Bus
FCL	Fully-Connected Layer
FDA	False Data Attack
FDI	False Data Injection
FDIA	False Data Injection Attack
FMA	Multi-Factor Authentication

GBM	Gradient Boosting Machine
GAN	Generative Adversarial Network
GMM	Gaussian Mixture Model
GN	Graph Network
GNN	Graph Neural Network
HAN	Home Area Network
HMAC	Hash-Based Message Authentication Code
ICS	Industrial Control System
IDS	Intrusion Detection System
IOT	Internet of Things
IS	Information Security
KM	Key Management
LCC	Line-Commutated Converter
LRA	Load Redistribution Attack
LSTM	Long Short-Term Memory
MA	Mutual Authentication
MG	MicroGrid
MICIE	Mission Critical Information Infrastructure Protection
ML	Machine Learning
MSVM	Multi-class Support Vector Machine
NAN	Neighborhood Area Network
NE	Nash Equilibrium
NN	Neural Network
NPP	Nuclear Power Plant
OPAL-RT	OPAL Real-Time Technologies
PG	Power Grid
PLC	Power Line Communication
PMU	Phase Measurement Unit
PS	Power System
PSES	Power System Energy Structure
PUF	Physical Unclonable Function
RCS	Robust Cramer Shoup
RE	Renewable Energy
ResNet	Residual Network
RNN	Recurrent Neural Network
SA	Security Architecture
SC	Smart City
SCADA	Supervisory Control and Data Acquisition
SCTP	Stream Control Transmission Protocol
SDN	Software Defined Networking
SFA	Single-Factor Authentication
SG	Smart Grid
SH	Smart Home
SM	Smart Meter
SN	Smart Network
SP	Service Provider
SS	Security Server
STPA	System-Theoretic Process Analysis
ST	Security Threat
SVM	Support Vector Machine
TA	Trusted Authority
TD	Time Delay
TDA	Theories of Defense and Attack
TTP	Trusted Third Party

WCTs	Wireless Communications Technologies
WiMAX	Worldwide Interoperability for Microwave Access
WLS	Weighted Least Square
WSN	Wireless Sensor Network
XML	Extensible Markup Language

References

1. Sankhwar, P. Energy reduction in residential housing units. *Int. J. Adv. Res. (Indore)* **2024**, *12*, 667–672. [CrossRef] [PubMed]
2. Mrabet, Z.E.; Kaabouch, N.; Ghazi, H.E.; Ghazi, H.E. Cyber-security in smart grid: Survey and challenges. *Comput. Electr. Eng.* **2018**, *67*, 469–482. [CrossRef]
3. Priyadarshini, I.; Kumar, R.; Sharma, R.; Singh, P.K.; Satapathy, S.C. Identifying cyber insecurities in trustworthy space and energy sector for smart grids. *Comput. Electr. Eng.* **2021**, *93*, 107204. [CrossRef]
4. Bekara, C. Security Issues and Challenges for the IoT-based Smart Grid. *Procedia Comput. Sci.* **2014**, *34*, 532–537. . [CrossRef]
5. Rani, S.; Kataria, A.; Chauhan, M.; Rattan, P.; Kumar, R.; Kumar Sivaraman, A. Security and Privacy Challenges in the Deployment of Cyber-Physical Systems in Smart City Applications: State-of-Art Work. *Mater. Today Proc.* **2022**, *62*, 4671–4676. . [CrossRef]
6. Sullivan, J.E.; Kamensky, D. How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid. *Electr. J.* **2017**, *30*, 30–35. [CrossRef]
7. Cowley, J.A.; Greitzer, F.L.; Woods, B. Effect of network infrastructure factors on information system risk judgments. *Comput. Secur.* **2015**, *52*, 142–158. [CrossRef]
8. Vitorino, J.; Praça, I.; Maia, E. SoK: Realistic adversarial attacks and defenses for intelligent network intrusion detection. *Comput. Secur.* **2023**, *134*, 103433. [CrossRef]
9. Liu, J.; Zhang, W.; Ma, T.; Tang, Z.; Xie, Y.; Gui, W.; Niyoyita, J.P. Toward security monitoring of industrial Cyber-Physical systems via hierarchically distributed intrusion detection. *Expert Syst. Appl.* **2020**, *158*, 113578. [CrossRef]
10. Research, E. Industroyer2: Industroyer Reloaded. 2022. Available online: https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ (accessed on 1 August 2024).
11. Reuters. Danish Energy Group Ørsted Says BlackCat Ransomware Gang Behind Cyberattack. 2023. Available online: https://www.reuters.com/technology/danish-energy-group-orsted-says-blackcat-ransomware-gang-behind-cyberattack-2023-11-20/ (accessed on 1 August 2024).
12. Kimani, K.; Oduol, V.; Langat, K. Cyber security challenges for IoT-based smart grid networks. *Int. J. Crit. Infrastruct. Prot.* **2019**, *25*, 36–49. [CrossRef]
13. Alsuwian, T.; Shahid Butt, A.; Amin, A.A. Smart Grid Cyber Security Enhancement: Challenges and Solutions—A Review. *Sustainability* **2022**, *14*, 4226. [CrossRef]
14. Ashibani, Y.; Mahmoud, Q.H. Cyber physical systems security: Analysis, challenges and solutions. *Comput. Secur.* **2017**, *68*, 81–97. [CrossRef]
15. Leszczyna, R. Cybersecurity and privacy in standards for smart grids – A comprehensive survey. *Comput. Stand. Interfaces* **2018**, *56*, 62–73. [CrossRef]
16. Colak, I.; Fulli, G.; Sagiroglu, S.; Yesilbudak, M.; Covrig, C.F. Smart grid projects in Europe: Current status, maturity and future scenarios. *Appl. Energy* **2015**, *152*, 58–70. [CrossRef]
17. Wang, D.; Wang, X.; Zhang, Y.; Jin, L. Detection of power grid disturbances and cyber-attacks based on machine learning. *J. Inf. Secur. Appl.* **2019**, *46*, 42–52. [CrossRef]
18. Yohanandhan, R.V.; Elavarasan, R.M.; Pugazhendhi, R.; Premkumar, M.; Mihet-Popa, L.; Terzija, V. A holistic review on Cyber-Physical Power System (CPPS) testbeds for secure and sustainable electric power grid—Part—I: Background on CPPS and necessity of CPPS testbeds. *Int. J. Electr. Power Energy Syst.* **2022**, *136*, 107718. [CrossRef]
19. Yoo, H.; Shon, T. Challenges and research directions for heterogeneous cyber–physical system based on IEC 61850: Vulnerabilities, security requirements, and security architecture. *Future Gener. Comput. Syst.* **2016**, *61*, 128–136. [CrossRef]
20. Hou, R.; Ren, G.; Zhou, C.; Yue, H.; Liu, H.; Liu, J. Analysis and research on network security and privacy security in ubiquitous electricity Internet of Things. *Comput. Commun.* **2020**, *158*, 64–72. [CrossRef]
21. Li, J.; Sun, C.; Su, Q. Analysis of cascading failures of power cyber-physical systems considering false data injection attacks. *Glob. Energy Interconnect.* **2021**, *4*, 204–213. [CrossRef]
22. Aoufi, S.; Derhab, A.; Guerroumi, M. Survey of false data injection in smart power grid: Attacks, countermeasures and challenges. *J. Inf. Secur. Appl.* **2020**, *54*, 102518. [CrossRef]
23. Tian, M.; Dong, Z.; Wang, X. Analysis of false data injection attacks in power systems: A dynamic Bayesian game-theoretic approach. *ISA Trans.* **2021**, *115*, 108–123. [CrossRef]
24. Xun, P.; dong Zhu, P.; Maharjan, S.; shuai Cui, P. Successive direct load altering attack in smart grid. *Comput. Secur.* **2018**, *77*, 79–93. [CrossRef]

25. Shin, J.; Choi, J.G.; Lee, J.W.; Lee, C.K.; Song, J.G.; Son, J.Y. Application of STPA-SafeSec for a cyber-attack impact analysis of NPPs with a condensate water system test-bed. *Nucl. Eng. Technol.* **2021**, *53*, 3319–3326. [CrossRef]
26. Vaccaro, A.; Pisica, I.; Lai, L.; Zobaa, A. A review of enabling methodologies for information processing in smart grids. *Int. J. Electr. Power Energy Syst.* **2019**, *107*, 516–522. [CrossRef]
27. Leszczyna, R. A review of standards with cybersecurity requirements for smart grid. *Comput. Secur.* **2018**, *77*, 262–276. [CrossRef]
28. Benz, M.; Chatterjee, D. Calculated risk? A cybersecurity evaluation tool for SMEs. *Bus. Horizons* **2020**, *63*, 531–540. [CrossRef]
29. Mahmood, A.; Javaid, N.; Razzaq, S. A review of wireless communications for smart grid. *Renew. Sustain. Energy Rev.* **2015**, *41*, 248–260. [CrossRef]
30. Colak, I.; Sagiroglu, S.; Fulli, G.; Yesilbudak, M.; Covrig, C.F. A survey on the critical issues in smart grid technologies. *Renew. Sustain. Energy Rev.* **2016**, *54*, 396–405. [CrossRef]
31. Mohammadpourfard, M.; Sami, A.; Seifi, A.R. A statistical unsupervised method against false data injection attacks: A visualization-based approach. *Expert Syst. Appl.* **2017**, *84*, 242–261. [CrossRef]
32. Pirbhulal, S.; Gkioulos, V.; Katsikas, S. A Systematic Literature Review on RAMS analysis for critical infrastructures protection. *Int. J. Crit. Infrastruct. Prot.* **2021**, *33*, 100427. [CrossRef]
33. Zhang, J. Distributed network security framework of energy internet based on internet of things. *Sustain. Energy Technol. Assess.* **2021**, *44*, 101051. [CrossRef]
34. Nafi, N.S.; Ahmed, K.; Gregory, M.A.; Datta, M. A survey of smart grid architectures, applications, benefits and standardization. *J. Netw. Comput. Appl.* **2016**, *76*, 23–36. [CrossRef]
35. Bretas, A.S.; Rossoni, A.; Trevizan, R.D.; Bretas, N.G. Distribution networks nontechnical power loss estimation: A hybrid data-driven physics model-based framework. *Electr. Power Syst. Res.* **2020**, *186*, 106397. [CrossRef]
36. Han, S.M.; Lee, C.; Seong, P.H. Estimating the frequency of cyber threats to nuclear power plants based on operating experience analysis. *Int. J. Crit. Infrastruct. Prot.* **2022**, *37*, 100523. [CrossRef]
37. Aly, M.; Khomh, F.; Haoues, M.; Quintero, A.; Yacout, S. Enforcing security in Internet of Things frameworks: A Systematic Literature Review. *Internet Things* **2019**, *6*, 100050. [CrossRef]
38. Otuoze, A.O.; Mustafa, M.W.; Larik, R.M. Smart grids security challenges: Classification by sources of threats. *J. Electr. Syst. Inf. Technol.* **2018**, *5*, 468–483. [CrossRef]
39. Langer, L.; Skopik, F.; Smith, P.; Kammerstetter, M. From old to new: Assessing cybersecurity risks for an evolving smart grid. *Comput. Secur.* **2016**, *62*, 165–176. [CrossRef]
40. Wang, W.; Lu, Z. Cyber security in the Smart Grid: Survey and challenges. *Comput. Netw.* **2013**, *57*, 1344–1371. [CrossRef]
41. Reka, S.S.; Dragicevic, T. Future effectual role of energy delivery: A comprehensive review of Internet of Things and smart grid. *Renew. Sustain. Energy Rev.* **2018**, *91*, 90–108. [CrossRef]
42. Axon, L.; Happa, J.; Goldsmith, M.; Creese, S. Hearing attacks in network data: An effectiveness study. *Comput. Secur.* **2019**, *83*, 367–388. [CrossRef]
43. Martinez-Pastor, B.; Nogal, M.; O'Connor, A.; Teixeira, R. Identifying critical and vulnerable links: A new approach using the Fisher information matrix. *Int. J. Crit. Infrastruct. Prot.* **2022**, *39*, 100570. [CrossRef]
44. Conti, S.; La Corte, A.; Nicolosi, R.; Rizzo, S. Impact of cyber-physical system vulnerability, telecontrol system availability and islanding on distribution network reliability. *Sustain. Energy Grids Netw.* **2016**, *6*, 143–151. [CrossRef]
45. Miller, T.; Staves, A.; Maesschalck, S.; Sturdee, M.; Green, B. Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems. *Int. J. Crit. Infrastruct. Prot.* **2021**, *35*, 100464. [CrossRef]
46. Rostami, A.; Mohammadi, M.; Karimipour, H. Reliability assessment of cyber-physical power systems considering the impact of predicted cyber vulnerabilities. *Int. J. Electr. Power Energy Syst.* **2023**, *147*, 108892. [CrossRef]
47. Christensen, D.; Martin, M.; Gantumur, E.; Mendrick, B. Risk Assessment at the Edge: Applying NERC CIP to Aggregated Grid-Edge Resources. *Electr. J.* **2019**, *32*, 50–57. [CrossRef]
48. Alkatheiri, M.S.; Chauhdary, S.H.; Alqarni, M.A. Seamless security apprise method for improving the reliability of sustainable energy-based smart home applications. *Sustain. Energy Technol. Assess.* **2021**, *45*, 101219. [CrossRef]
49. Saeh, I.; Mustafa, M.; Mohammed, Y.; Almaktar, M. Static Security classification and Evaluation classifier design in electric power grid with presence of PV power plants using C-4.5. *Renew. Sustain. Energy Rev.* **2016**, *56*, 283–290. [CrossRef]
50. Leszczyna, R. Standards on cyber security assessment of smart grid. *Int. J. Crit. Infrastruct. Prot.* **2018**, *22*, 70–89. [CrossRef]
51. Zografopoulos, I.; Kuruvila, A.P.; Basu, K.; Konstantinou, C. Time series-based detection and impact analysis of firmware attacks in microgrids. *Energy Rep.* **2022**, *8*, 11221–11234. [CrossRef]
52. Lee, L.; Hu, P. Vulnerability analysis of cascading dynamics in smart grids under load redistribution attacks. *Int. J. Electr. Power Energy Syst.* **2019**, *111*, 182–190. [CrossRef]
53. Wei, M.; Wang, W. Data-centric threats and their impacts to real-time communications in smart grid. *Comput. Netw.* **2016**, *104*, 174–188. [CrossRef]

54. Sakhnini, J.; Karimipour, H.; Dehghantanha, A.; Parizi, R.M.; Srivastava, G. Security aspects of Internet of Things aided smart grids: A bibliometric survey. *Internet Things* **2021**, *14*, 100111. [CrossRef]
55. Hussain, S.; Hernandez Fernandez, J.; Al-Ali, A.K.; Shikfa, A. Vulnerabilities and countermeasures in electrical substations. *Int. J. Crit. Infrastruct. Prot.* **2021**, *33*, 100406. [CrossRef]
56. Huang, B.; Li, Y.; Zhan, F.; Sun, Q.; Zhang, H. A Distributed Robust Economic Dispatch Strategy for Integrated Energy System Considering Cyber-Attacks. *IEEE Trans. Ind. Inform.* **2021**, *18*, 880–890. [CrossRef]
57. Zhang, S.; Zhang, X.; Zhang, R.; Gu, W.; Cao, G. N-1 Evaluation of Integrated Electricity and Gas System Considering Cyber-Physical Interdependence. *IEEE Trans. Smart Grid* **2025**, *16*, 3728–3742. [CrossRef]
58. Guan, Z.; Lu, X.; Yang, W.; Wu, L.; Wang, N.; Zhang, Z. Achieving efficient and Privacy-preserving energy trading based on blockchain and ABE in smart grid. *J. Parallel Distrib. Comput.* **2021**, *147*, 34–45. [CrossRef]
59. Tolba, A.; Al-Makhadmeh, Z. A cybersecurity user authentication approach for securing smart grid communications. *Sustain. Energy Technol. Assess.* **2021**, *46*, 101284. [CrossRef]
60. Saqib, M.; Jasra, B.; Moon, A.H. A lightweight three factor authentication framework for IoT based critical applications. *J. King Saud Univ.—Comput. Inf. Sci.* **2022**, *34*, 6925–6937. [CrossRef]
61. Jie, X.; Wang, H.; Fei, M.; Du, D.; Sun, Q.; Yang, T. Anomaly behavior detection and reliability assessment of control systems based on association rules. *Int. J. Crit. Infrastruct. Prot.* **2018**, *22*, 90–99. [CrossRef]
62. Ferrag, M.A.; Babaghayou, M.; Yazici, M.A. Cyber security for fog-based smart grid SCADA systems: Solutions and challenges. *J. Inf. Secur. Appl.* **2020**, *52*, 102500. [CrossRef]
63. Moussaoui, B.; Chikouche, N.; Fouchal, H. An efficient privacy scheme for C-ITS stations. *Comput. Electr. Eng.* **2023**, *107*, 108613. [CrossRef]
64. Wang, Z.; Jiang, D.; Wang, F.; Lv, Z.; Nowak, R. A polymorphic heterogeneous security architecture for edge-enabled smart grids. *Sustain. Cities Soc.* **2021**, *67*, 102661. [CrossRef]
65. Kong, W.; Shen, J.; Vijayakumar, P.; Cho, Y.; Chang, V. A practical group blind signature scheme for privacy protection in smart grid. *J. Parallel Distrib. Comput.* **2020**, *136*, 29–39. [CrossRef]
66. Sadhukhan, D.; Ray, S.; Obaidat, M.S.; Dasgupta, M. A secure and privacy preserving lightweight authentication scheme for smart-grid communication using elliptic curve cryptography. *J. Syst. Archit.* **2021**, *114*, 101938. [CrossRef]
67. Irshad, A.; Chaudhry, S.A.; Alazab, M.; Kanwal, A.; Sultan Zia, M.; Zikria, Y.B. A secure demand response management authentication scheme for smart grid. *Sustain. Energy Technol. Assess.* **2021**, *48*, 101571. [CrossRef]
68. Zhang, H.; Wang, J.; Ding, Y. Blockchain-based decentralized and secure keyless signature scheme for smart grid. *Energy* **2019**, *180*, 955–967. [CrossRef]
69. Sharma, V.; You, I.; Jayakody, D.N.K.; Atiquzzaman, M. Cooperative trust relaying and privacy preservation via edge-crowdsourcing in social Internet of Things. *Future Gener. Comput. Syst.* **2019**, *92*, 758–776. [CrossRef]
70. Singh, N.K.; Mahajan, V. End-User Privacy Protection Scheme from cyber intrusion in smart grid advanced metering infrastructure. *Int. J. Crit. Infrastruct. Prot.* **2021**, *34*, 100410. [CrossRef]
71. Cui, H. Handoff control strategy of cyber physical systems under dynamic data attack. *Comput. Commun.* **2021**, *178*, 183–190. [CrossRef]
72. Adamsky, F.; Aubigny, M.; Battisti, F.; Carli, M.; Cimorelli, F.; Cruz, T.; Di Giorgio, A.; Foglietta, C.; Galli, A.; Giuseppi, A.; et al. Integrated protection of industrial control systems from cyber-attacks: The ATENA approach. *Int. J. Crit. Infrastruct. Prot.* **2018**, *21*, 72–82. [CrossRef]
73. Li, Q.; Li, A.; Wang, T.; Cai, Y. Interconnected hybrid AC-DC microgrids security enhancement using blockchain technology considering uncertainty. *Int. J. Electr. Power Energy Syst.* **2021**, *133*, 107324. [CrossRef]
74. Khan, A.A.; Kumar, V.; Ahmad, M.; Rana, S. LAKAF: Lightweight authentication and key agreement framework for smart grid network. *J. Syst. Archit.* **2021**, *116*, 102053. [CrossRef]
75. Gope, P.; Amin, R.; Hafizul Islam, S.; Kumar, N.; Bhalla, V.K. Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. *Future Gener. Comput. Syst.* **2018**, *83*, 629–637. [CrossRef]
76. Zhou, L.; Li, X.; Yeh, K.H.; Su, C.; Chiu, W. Lightweight IoT-based authentication scheme in cloud computing circumstance. *Future Gener. Comput. Syst.* **2019**, *91*, 244–251. [CrossRef]
77. Khazaei, J.; Amini, M.H. Protection of large-scale smart grids against false data injection cyberattacks leading to blackouts. *Int. J. Crit. Infrastruct. Prot.* **2021**, *35*, 100457. [CrossRef]
78. Malik, K.R.; Farhan, M.; Habib, M.A.; Khalid, S.; Ahmad, M.; Ghafir, I. Remote access capability embedded in linked data using bi-directional transformation: Issues and simulation. *Sustain. Cities Soc.* **2018**, *38*, 662–674. [CrossRef]
79. Abou el Kalam, A. Securing SCADA and critical industrial systems: From needs to security mechanisms. *Int. J. Crit. Infrastruct. Prot.* **2021**, *32*, 100394. [CrossRef]

80. Ostad-Sharif, A.; Arshad, H.; Nikooghadam, M.; Abbasinezhad-Mood, D. Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme. *Future Gener. Comput. Syst.* **2019**, *100*, 882–892. [CrossRef]
81. Hasan, R.; Khan, R. Unified authentication factors and fuzzy service access using interaction provenance. *Comput. Secur.* **2017**, *67*, 211–231. [CrossRef]
82. Moghadam, M.F.; Nikooghadam, M.; Mohajerzadeh, A.H.; Movali, B. A lightweight key management protocol for secure communication in smart grids. *Electr. Power Syst. Res.* **2020**, *178*, 106024. [CrossRef]
83. Chaudhry, S.A.; Shon, T.; Al-Turjman, F.; Alsharif, M.H. Correcting design flaws: An improved and cloud assisted key agreement scheme in cyber physical systems. *Comput. Commun.* **2020**, *153*, 527–537. [CrossRef]
84. Haseeb, K.; Siraj, M.; Alzahrani, F.A.; ullah, Z.; Jeon, G. Sensor-based optimization multi-decision model for sustainable smart cities. *Sustain. Energy Technol. Assess.* **2023**, *60*, 103452. [CrossRef]
85. Rao, A.S.V.; Roy, P.K.; Amgoth, T.; Bhattacharya, A. A deep learning-based authentication protocol for IoT-enabled LTE systems. *Future Gener. Comput. Syst.* **2024**, *154*, 451–464. [CrossRef]
86. Singh, I.; Singh, B. Access management of IoT devices using access control mechanism and decentralized authentication: A review. *Meas. Sens.* **2023**, *25*, 100591. [CrossRef]
87. Mbarek, B.; Ge, M.; Pitner, T. An Efficient Mutual Authentication Scheme for Internet of Things. *Internet Things* **2020**, *9*, 100160. [CrossRef]
88. Smith-Creasey, M.; Rajarajan, M. A novel word-independent gesture-typing continuous authentication scheme for mobile devices. *Comput. Secur.* **2019**, *83*, 140–150. [CrossRef]
89. Velásquez, I.; Caro, A.; Rodríguez, A. Authentication schemes and methods: A systematic literature review. *Inf. Softw. Technol.* **2018**, *94*, 30–37. [CrossRef]
90. Yang, H.; Guo, Y.; Guo, Y. Blockchain-based cloud-fog collaborative smart home authentication scheme. *Comput. Netw.* **2024**, *242*, 110240. [CrossRef]
91. Alzubi, J.A. Blockchain-based Lamport Merkle Digital Signature: Authentication tool in IoT healthcare. *Comput. Commun.* **2021**, *170*, 200–208. [CrossRef]
92. ul Haq, M.E.; Awais Azam, M.; Naeem, U.; Amin, Y.; Loo, J. Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing. *J. Netw. Comput. Appl.* **2018**, *109*, 24–35. [CrossRef]
93. Sadhukhan, D.; Ray, S.; Dasgupta, M.; Khan, M.K. Development of a provably secure and privacy-preserving lightweight authentication scheme for roaming services in global mobility network. *J. Netw. Comput. Appl.* **2024**, *224*, 103831. [CrossRef]
94. Lee, T.F.; Lou, D.C.; Chang, C.H. Enhancing lightweight authenticated key agreement with privacy protection using dynamic identities for Internet of Drones. *Internet Things* **2023**, *23*, 100877. [CrossRef]
95. Harbi, Y.; Aliouat, Z.; Harous, S.; Gueroui, A.M. Lightweight blockchain-based remote user authentication for fog-enabled IoT deployment. *Comput. Commun.* **2024**, *221*, 90–105. [CrossRef]
96. Ibrahim, O.A.; Sciancalepore, S.; Di Pietro, R. MAG-PUFs: Authenticating IoT devices via electromagnetic physical unclonable functions and deep learning. *Comput. Secur.* **2024**, *143*, 103905. [CrossRef]
97. Aldosary, A.; Tanveer, M. PAAF-SHS: PUF and authenticated encryption based authentication framework for the IoT-enabled smart healthcare system. *Internet Things* **2024**, *26*, 101159. [CrossRef]
98. Mardi, F.Z.; Hadjadj-Aoul, Y.; Bagaa, M.; Benamar, N. Resource Allocation for LoRaWAN Network Slicing: Multi-Armed Bandit-based Approaches. *Internet Things* **2024**, *26*, 101195. [CrossRef]
99. Bahache, A.N.; Chikouche, N.; Akleylek, S. Securing Cloud-based Healthcare Applications with a Quantum-resistant Authentication and Key Agreement Framework. *Internet Things* **2024**, *26*, 101200. [CrossRef]
100. Zhu, L.; Tan, L. Task offloading scheme of vehicular cloud edge computing based on Digital Twin and improved A3C. *Internet Things* **2024**, *26*, 101192. [CrossRef]
101. Wang, Y.; Xing, A.; Qu, Z.; Han, X.; Dong, H.; Georgievitch, P.M. False data injection attack detection based on interval affine state estimation. *Electr. Power Syst. Res.* **2022**, *210*, 108100. [CrossRef]
102. Haes Alhelou, H.; Hamedani Golshan, M.; Askari-Marnani, J. Robust sensor fault detection and isolation scheme for interconnected smart power systems in presence of RER and EVs using unknown input observer. *Int. J. Electr. Power Energy Syst.* **2018**, *99*, 682–694. [CrossRef]
103. Nazir, S.; Patel, S.; Patel, D. Assessing and augmenting SCADA cyber security: A survey of techniques. *Comput. Secur.* **2017**, *70*, 436–454. [CrossRef]
104. Sengan, S.; V, S.; V, I.; Velayutham, P.; Ravi, L. Detection of false data cyber-attacks for the assessment of security in smart grid using deep learning. *Comput. Electr. Eng.* **2021**, *93*, 107211. [CrossRef]
105. Fadel, E.; Gungor, V.; Nassef, L.; Akkari, N.; Malik, M.A.; Almasri, S.; Akyildiz, I.F. A survey on wireless sensor networks for smart grid. *Comput. Commun.* **2015**, *71*, 22–33. [CrossRef]

106. Bera, B.; Sikdar, B. Securing Post-Quantum Communication for Smart Grid Applications. In Proceedings of the 2024 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Oslo, Norway, 17–20 September 2024; pp. 555–561. [CrossRef]
107. Gharavi, H.; Granjal, J.; Monteiro, E. Post-Quantum Blockchain Security for the Internet of Things: Survey and Research Directions. *IEEE Commun. Surv. Tutor.* **2024**, *26*, 1748–1774. [CrossRef]
108. Hamdi, N. A hybrid learning technique for intrusion detection system for smart grid. *Sustain. Comput. Inform. Syst.* **2025**, *46*, 101102. [CrossRef]
109. Lazzarini, R.; Tianfield, H.; Charissis, V. Federated Learning for IoT Intrusion Detection. *AI* **2023**, *4*, 509–530. [CrossRef]
110. Alqahtani, H.; Kumar, G. Cybersecurity in Electric and Flying Vehicles: Threats, Challenges, AI Solutions & Future Directions. *ACM Comput. Surv.* **2024**, *57*. [CrossRef]
111. Ronanki, D.; Karneddi, H. Electric Vehicle Charging Infrastructure: Review, Cyber Security Considerations, Potential Impacts, Countermeasures, and Future Trends. *IEEE J. Emerg. Sel. Top. Power Electron.* **2024**, *12*, 242–256. [CrossRef]
112. Alhasnawi, B.N.; Jasim, B.H. A new internet of things enabled trust distributed demand side management system. *Sustain. Energy Technol. Assess.* **2021**, *46*, 101272. [CrossRef]
113. Sundararaj, V.; Muthukumar, S.; Kumar, R. An optimal cluster formation based energy efficient dynamic scheduling hybrid MAC protocol for heavy traffic load in wireless sensor networks. *Comput. Secur.* **2018**, *77*, 277–288. [CrossRef]
114. Alam, S.; Sohail, M.F.; Ghauri, S.A.; Qureshi, I.; Aqdas, N. Cognitive radio based Smart Grid Communication Network. *Renew. Sustain. Energy Rev.* **2017**, *72*, 535–548. [CrossRef]
115. Li, Q.; Yue, Y.; Wang, Z. Deep Robust Cramer Shoup Delay Optimized Fully Homomorphic For IIOT secured transmission in cloud computing. *Comput. Commun.* **2020**, *161*, 10–18. [CrossRef]
116. Nuñez, D.; Fernández-Gago, C.; Luna, J. Eliciting metrics for accountability of cloud systems. *Comput. Secur.* **2016**, *62*, 149–164. [CrossRef]
117. Liu, Y.; Zhang, S. Information security and storage of Internet of Things based on block chains. *Future Gener. Comput. Syst.* **2020**, *106*, 296–303. [CrossRef]
118. Iqbal, A.; Ullah, F.; Anwar, H.; Kwak, K.S.; Imran, M.; Jamal, W.; ur Rahman, A. Interoperable Internet-of-Things platform for smart home system using Web-of-Objects and cloud. *Sustain. Cities Soc.* **2018**, *38*, 636–646. [CrossRef]
119. Einspieler, S.; Steinwender, B.; Elmenreich, W. Mixed-triggered communication with limited elastic slot boundaries. *Microprocess. Microsystems* **2021**, *86*, 104323. [CrossRef]
120. Bouabdellah, M.; Kaabouch, N.; El Bouanani, F.; Ben-Azza, H. Network layer attacks and countermeasures in cognitive radio networks: A survey. *J. Inf. Secur. Appl.* **2018**, *38*, 40–49. [CrossRef]
121. Liu, M.; Lei, W.; Sun, J.; Lei, H.; Tang, H. Power and rate control in wireless communication systems with energy harvesting and rateless codes. *Phys. Commun.* **2023**, *59*, 102083. [CrossRef]
122. Sharma, K.; Saini, L.M. Power-line communications for smart grid: Progress, challenges, opportunities and status. *Renew. Sustain. Energy Rev.* **2017**, *67*, 704–751. [CrossRef]
123. Yigit, M.; Gungor, V.C.; Tuna, G.; Rangoussi, M.; Fadel, E. Power line communication technologies for smart grid applications: A review of advances and challenges. *Comput. Netw.* **2014**, *70*, 366–383. [CrossRef]
124. Bae, M.; Kim, K.; Kim, H. Preserving privacy and efficiency in data communication and aggregation for AMI network. *J. Netw. Comput. Appl.* **2016**, *59*, 333–344. [CrossRef]
125. Jha, A.V.; Appasani, B.; Ustun, T.S. Resiliency assessment methodology for synchrophasor communication networks in a smart grid cyber–physical system. *Energy Rep.* **2022**, *8*, 1108–1115. [CrossRef]
126. Tsado, Y.; Lund, D.; Gamage, K.A. Resilient communication for smart grid ubiquitous sensor network: State of the art and prospects for next generation. *Comput. Commun.* **2015**, *71*, 34–49. [CrossRef]
127. Wang, W.; Harrou, F.; Bouyeddou, B.; Senouci, S.M.; Sun, Y. Cyber-attacks detection in industrial systems using artificial intelligence-driven methods. *Int. J. Crit. Infrastruct. Prot.* **2022**, *38*, 100542. [CrossRef]
128. Cui, L.; Qu, Y.; Gao, L.; Xie, G.; Yu, S. Detecting false data attacks using machine learning techniques in smart grid: A survey. *J. Netw. Comput. Appl.* **2020**, *170*, 102808. [CrossRef]
129. Elsisi, M.; Su, C.L.; ALI, M. Design of Reliable IoT Systems with Deep Learning to Support Resilient Demand Side Management in Smart Grids Against Adversarial Attacks. *IEEE Trans. Ind. Appl.* **2023**, *60*, 2095–2106. [CrossRef]
130. Chen, D.; Wawrzynski, P.; Lv, Z. Cyber security in smart cities: A review of deep learning-based applications and case studies. *Sustain. Cities Soc.* **2021**, *66*, 102655. [CrossRef]
131. Attia, M.; Senouci, S.M.; Sedjelmaci, H.; Aglzim, E.H.; Chrenko, D. An efficient Intrusion Detection System against cyber-physical attacks in the smart grid. *Comput. Electr. Eng.* **2018**, *68*, 499–512. [CrossRef]
132. Liu, C.; Xi, J.; Hao, Q.; Li, J.; Wang, J.; Dong, H.; Su, C. Grid-Forming Converter Overcurrent Limiting Strategy Based on Additional Current Loop. *Electronics* **2023**, *12*, 1112. [CrossRef]

133. Wang, H.; Ruan, J.; Ma, Z.; Zhou, B.; Fu, X.; Cao, G. Deep learning aided interval state prediction for improving cyber security in energy internet. *Energy* **2019**, *174*, 1292–1304. [CrossRef]
134. Teng, T.; Ma, L. Deep learning-based risk management of financial market in smart grid. *Comput. Electr. Eng.* **2022**, *99*, 107844. [CrossRef]
135. Xie, G.; Chen, X.; Weng, Y. Input modeling and uncertainty quantification for improving volatile residential load forecasting. *Energy* **2020**, *211*, 119007. [CrossRef]
136. Berghout, T.; Benbouzid, M. EL-NAHL: Exploring labels autoencoding in augmented hidden layers of feedforward neural networks for cybersecurity in smart grids. *Reliab. Eng. Syst. Saf.* **2022**, *226*, 108680. [CrossRef]
137. Khan, A.A.; Beg, O.A.; Alamaniotis, M.; Ahmed, S. Intelligent anomaly identification in cyber-physical inverter-based systems. *Electr. Power Syst. Res.* **2021**, *193*, 107024. [CrossRef]
138. Nawaz, R.; Akhtar, R.; Shahid, M.A.; Qureshi, I.M.; Mahmood, M.H. Machine learning based false data injection in smart grid. *Int. J. Electr. Power Energy Syst.* **2021**, *130*, 106819. [CrossRef]
139. Rouzbahani, H.M.; Karimipour, H.; Lei, L. Multi-layer defense algorithm against deep reinforcement learning-based intruders in smart grids. *Int. J. Electr. Power Energy Syst.* **2023**, *146*, 108798. [CrossRef]
140. Sakhnini, J.; Karimipour, H.; Dehghantanha, A.; Parizi, R.M. Physical layer attack identification and localization in cyber–physical grid: An ensemble deep learning based approach. *Phys. Commun.* **2021**, *47*, 101394. [CrossRef]
141. Huda, S.; Yearwood, J.; Hassan, M.M.; Almogren, A. Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks. *Appl. Soft Comput.* **2018**, *71*, 66–77. [CrossRef]
142. Shafiq, M.; Tian, Z.; Sun, Y.; Du, X.; Guizani, M. Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city. *Future Gener. Comput. Syst.* **2020**, *107*, 433–442. [CrossRef]
143. Valueian, M.; Vahidi-Asl, M.; Khalilian, A. SituRepair: Incorporating machine-learning fault class prediction to inform situational multiple fault automatic program repair. *Int. J. Crit. Infrastruct. Prot.* **2022**, *37*, 100527. [CrossRef]
144. Singh, N.K.; Majeed, M.A.; Mahajan, V. Statistical machine learning defensive mechanism against cyber intrusion in smart grid cyber-physical network. *Comput. Secur.* **2022**, *123*, 102941. [CrossRef]
145. S, S.; D, P.W. An enhanced optimization based algorithm for intrusion detection in SCADA network. *Comput. Secur.* **2017**, *70*, 16–26. [CrossRef]
146. Yi, P.; Zhu, T.; Zhang, Q.; Wu, Y.; Pan, L. Puppet attack: A denial of service attack in advanced metering infrastructure network. *J. Netw. Comput. Appl.* **2016**, *59*, 325–332. [CrossRef]
147. Chen, Z.; Yeo, C.K.; Lee, B.S.; Lau, C.T. Detection of network anomalies using Improved-MSPCA with sketches. *Comput. Secur.* **2017**, *65*, 314–328. [CrossRef]
148. Kreimel, P.; Eigner, O.; Mercaldo, F.; Santone, A.; Tavolato, P. Anomaly detection in substation networks. *J. Inf. Secur. Appl.* **2020**, *54*, 102527. [CrossRef]
149. Shen, Z.; Xu, W.; Li, W.; Shi, Y.; Gao, F. Digital twin application for attach detection and mitigation of PV-based smart systems using fast and accurate hybrid machine learning algorithm. *Sol. Energy* **2023**, *250*, 377–387. [CrossRef]
150. Xiang, Y.; Wang, L. A game-theoretic study of load redistribution attack and defense in power systems. *Electr. Power Syst. Res.* **2017**, *151*, 12–25. [CrossRef]
151. Zarreh, A.; Saygin, C.; Wan, H.; Lee, Y.; Bracho, A. A game theory based cybersecurity assessment model for advanced manufacturing systems. *Procedia Manuf.* **2018**, *26*, 1255–1264. [CrossRef]
152. Davarikia, H.; Barati, M.; Al-Assad, M.; Chan, Y. A novel approach in strategic planning of power networks against physical attacks. *Electr. Power Syst. Res.* **2020**, *180*, 106140. [CrossRef]
153. Cifranic, N.; Hallman, R.A.; Romero-Mariona, J.; Souza, B.; Calton, T.; Coca, G. Decepti-SCADA: A cyber deception framework for active defense of networked critical infrastructures. *Internet Things* **2020**, *12*, 100320. [CrossRef]
154. Zhang, G.; Li, J.; Bamisile, O.; Cai, D.; Huang, Q. A novel data-driven time-delay attack evaluation method for wide-area cyber–physical smart grid systems. *Sustain. Energy Grids Netw.* **2022**, *32*, 100960. [CrossRef]
155. Yi, N.; Wang, Q.; Yan, L.; Tang, Y.; Xu, J. A multi-stage game model for the false data injection attack from attacker's perspective. *Sustain. Energy Grids Netw.* **2021**, *28*, 100541. [CrossRef]
156. Wang, X.; Luo, X.; Zhang, M.; Guan, X. Distributed detection and isolation of false data injection attacks in smart grids via nonlinear unknown input observers. *Int. J. Electr. Power Energy Syst.* **2019**, *110*, 208–222. [CrossRef]
157. Mukherjee, D. A novel strategy for locational detection of false data injection attack. *Sustain. Energy Grids Netw.* **2022**, *31*, 100702. [CrossRef]
158. Liu, T.; Sun, Y.; Liu, Y.; Gui, Y.; Zhao, Y.; Wang, D.; Shen, C. Abnormal traffic-indexed state estimation: A cyber–physical fusion approach for Smart Grid attack detection. *Future Gener. Comput. Syst.* **2015**, *49*, 94–103. [CrossRef]
159. Sreeram, T.; Krishna, S. A novel vulnerability index to select measurements for defense against false data injection attacks. *Int. J. Electr. Power Energy Syst.* **2023**, *145*, 108626. [CrossRef]

160. Rizvi, S.; Orr, R.; Cox, A.; Ashokkumar, P.; Rizvi, M.R. Identifying the attack surface for IoT network. *Internet Things* **2020**, *9*, 100162. [CrossRef]
161. Nam, J.; Park, G.; Kim, T.; Shim, H. A Posteriori Detection of Moment of Attack on Cyber-physical Systems: A Back-and-forth Observer Approach. *IFAC-PapersOnLine* **2018**, *51*, 188–193. . [CrossRef]
162. Rahiminejad, A.; Plotnek, J.; Atallah, R.; Dubois, M.A.; Malatrait, D.; Ghafouri, M.; Mohammadi, A.; Debbabi, M. A resilience-based recovery scheme for smart grid restoration following cyberattacks to substations. *Int. J. Electr. Power Energy Syst.* **2023**, *145*, 108610. [CrossRef]
163. Teixeira, A.; Shames, I.; Sandberg, H.; Johansson, K.H. A secure control framework for resource-limited adversaries. *Automatica* **2015**, *51*, 135–148. [CrossRef]
164. He, H.; Huang, S.; Liu, Y.; Zhang, T. A tri-level optimization model for power grid defense with the consideration of post-allocated DGs against coordinated cyber-physical attacks. *Int. J. Electr. Power Energy Syst.* **2021**, *130*, 106903. [CrossRef]
165. Xiang, Y.; Wang, L.; Liu, N. Coordinated attacks on electric power systems in a cyber-physical environment. *Electr. Power Syst. Res.* **2017**, *149*, 156–168. [CrossRef]
166. Lai, K.; Illindala, M.; Subramaniam, K. A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyber-physical environment. *Appl. Energy* **2019**, *235*, 204–218. [CrossRef]
167. Coppolino, L.; Antonio, S.D.; Romano, L. Exposing vulnerabilities in electric power grids: An experimental approach. *Int. J. Crit. Infrastruct. Prot.* **2014**, *7*, 51–60. [CrossRef]
168. Alexopoulos, T.A.; Korres, G.N.; Manousakis, N.M. Complementarity reformulations for false data injection attacks on PMU-only state estimation. *Electr. Power Syst. Res.* **2020**, *189*, 106796. [CrossRef]
169. Khazaei, J. Cyberattacks with limited network information leading to transmission line overflow in cyber–physical power systems. *Sustain. Energy Grids Netw.* **2021**, *27*, 100505. [CrossRef]
170. Giglou, P.A.; Najafi Ravadanegh, S. Defending against false data injection attack on demand response program: A bi-level strategy. *Sustain. Energy Grids Netw.* **2021**, *27*, 100506. [CrossRef]
171. Li, Y.; Wang, Y. Developing graphical detection techniques for maintaining state estimation integrity against false data injection attack in integrated electric cyber-physical system. *J. Syst. Archit.* **2020**, *105*, 101705. [CrossRef]
172. Lee, C.; Han, S.M.; Chae, Y.H.; Seong, P.H. Development of a cyberattack response planning method for nuclear power plants by using the Markov decision process model. *Ann. Nucl. Energy* **2022**, *166*, 108725. [CrossRef]
173. Lee, C.; Ho Chae, Y.; Hyun Seong, P. Development of a method for estimating security state: Supporting integrated response to cyber-attacks in NPPs. *Ann. Nucl. Energy* **2021**, *158*, 108287. [CrossRef]
174. Kalech, M. Cyber-attack detection in SCADA systems using temporal pattern recognition techniques. *Comput. Secur.* **2019**, *84*, 225–238. [CrossRef]
175. Gallo, A.J.; Turan, M.S.; Boem, F.; Ferrari-Trecate, G.; Parisini, T. Distributed watermarking for secure control of microgrids under replay attacks. *IFAC-PapersOnLine* **2018**, *51*, 182–187. [CrossRef]
176. Ding, Z.; Chen, C.; Cui, M.; Bi, W.; Chen, Y.; Li, F. Dynamic game-based defensive primary frequency control system considering intelligent attackers. *Reliab. Eng. Syst. Saf.* **2021**, *216*, 107966. [CrossRef]
177. Mohammadpourfard, M.; Weng, Y.; Pechenizkiy, M.; Tajdinian, M.; Mohammadi-Ivatloo, B. Ensuring cybersecurity of smart grid against data integrity attacks under concept drift. *Int. J. Electr. Power Energy Syst.* **2020**, *119*, 105947. [CrossRef]
178. Su, J.; He, S.; Wu, Y. Features selection and prediction for IoT attacks. *High-Confid. Comput.* **2022**, *2*, 100047. [CrossRef]
179. Bretas, A.S.; Bretas, N.G.; Carvalho, B.E. Further contributions to smart grids cyber-physical security as a malicious data attack: Proof and properties of the parameter error spreading out to the measurements and a relaxed correction model. *Int. J. Electr. Power Energy Syst.* **2019**, *104*, 43–51. [CrossRef]
180. Nishino, H.; Ishii, H. Distributed Detection of Cyber Attacks and Faults for Power Systems. *IFAC Proc. Vol.* **2014**, *47*, 11932–11937. [CrossRef]
181. Lin, W.T.; Chen, G.; Huang, Y. Incentive edge-based federated learning for false data injection attack detection on power grid state estimation: A novel mechanism design approach. *Appl. Energy* **2022**, *314*, 118828. [CrossRef]
182. Ashrafuzzaman, M.; Das, S.; Chakhchoukh, Y.; Shiva, S.; Sheldon, F.T. Detecting stealthy false data injection attacks in the smart grid using ensemble-based machine learning. *Comput. Secur.* **2020**, *97*, 101994. [CrossRef]
183. Shi, H.; Xie, L.; Peng, L. Detection of false data injection attacks in smart grid based on a new dimensionality-reduction method. *Comput. Electr. Eng.* **2021**, *91*, 107058. [CrossRef]
184. Rice, E.B.; AlMajali, A. Mitigating the Risk of Cyber Attack on Smart Grid Systems. *Procedia Comput. Sci.* **2014**, *28*, 575–582. [CrossRef]
185. Ayad, A.; Khalaf, M.; Salama, M.; El-Saadany, E.F. Mitigation of false data injection attacks on automatic generation control considering nonlinearities. *Electr. Power Syst. Res.* **2022**, *209*, 107958. [CrossRef]

186. Song, C.; Sun, Y.; Han, G.; Rodrigues, J.J. Intrusion detection based on hybrid classifiers for smart grid. *Comput. Electr. Eng.* **2021**, *93*, 107212. [CrossRef]
187. Margossian, H.; Sayed, M.A.; Fawaz, W.; Nakad, Z. Partial grid false data injection attacks against state estimation. *Int. J. Electr. Power Energy Syst.* **2019**, *110*, 623–629. [CrossRef]
188. Cheng, Z.; Yue, D.; Hu, S.; Huang, C.; Dou, C.; Chen, L. Resilient load frequency control design: DoS attacks against additional control loop. *Int. J. Electr. Power Energy Syst.* **2020**, *115*, 105496. [CrossRef]
189. Warraich, Z.; Morsi, W. Early detection of cyber–physical attacks on fast charging stations using machine learning considering vehicle-to-grid operation in microgrids. *Sustain. Energy Grids Netw.* **2023**, *34*, 101027. [CrossRef]
190. Yurekten, O.; Demirci, M. SDN-based cyber defense: A survey. *Future Gener. Comput. Syst.* **2021**, *115*, 126–149. [CrossRef]
191. Khan, S.; Akhunzada, A. A hybrid DL-driven intelligent SDN-enabled malware detection framework for Internet of Medical Things (IoMT). *Comput. Commun.* **2021**, *170*, 209–216. [CrossRef]
192. Bretas, A.S.; Bretas, N.G.; Carvalho, B.; Baeyens, E.; Khargonekar, P.P. Smart grids cyber-physical security as a malicious data attack: An innovation approach. *Electr. Power Syst. Res.* **2017**, *149*, 210–219. [CrossRef]
193. Raghunath Kumar Babu, D.; Packialatha, A. Hybrid classification model with tuned weight for cyber attack detection: Big data perspective. *Adv. Eng. Softw.* **2023**, *177*, 103408. [CrossRef]
194. Zou, T.; Bretas, A.S.; Ruben, C.; Dhulipala, S.C.; Bretas, N. Smart grids cyber-physical security: Parameter correction model against unbalanced false data injection attacks. *Electr. Power Syst. Res.* **2020**, *187*, 106490. [CrossRef]
195. Qiu, W.; Sun, K.; Yao, W.; You, S.; Yin, H.; Ma, X.; Liu, Y. Time-frequency based cyber security defense of wide-area control system for fast frequency reserve. *Int. J. Electr. Power Energy Syst.* **2021**, *132*, 107151. [CrossRef]
196. Li, G.; Jiang, S.; Xin, Y.; Wang, Z.; Wang, L.; Wu, X.; Li, X. An improved DIM interface algorithm for the MMC-HVDC power hardware-in-the-loop simulation system. *Int. J. Electr. Power Energy Syst.* **2018**, *99*, 69–78. [CrossRef]
197. Fattahi, J.; Wright, D.; Schriemer, H. An energy internet DERMS platform using a multi-level Stackelberg game. *Sustain. Cities Soc.* **2020**, *60*, 102262. [CrossRef]
198. Cui, Q.; Weng, Y. An environment-adaptive protection scheme with long-term reward for distribution networks. *Int. J. Electr. Power Energy Syst.* **2021**, *124*, 106350. [CrossRef]
199. Akkad, A.; Wills, G.; Rezazadeh, A. An information security model for an IoT-enabled Smart Grid in the Saudi energy sector. *Comput. Electr. Eng.* **2023**, *105*, 108491. [CrossRef]
200. Sun, Z.; Cai, G.; Yang, D.; Liu, C. Application of power system energy structures to track dominated oscillation paths and generator damping contribution during low-frequency oscillations. *Int. J. Electr. Power Energy Syst.* **2019**, *104*, 52–68. [CrossRef]
201. Barbosa, P.; Brito, A.; Almeida, H. A Technique to provide differential privacy for appliance usage in smart metering. *Inf. Sci.* **2016**, *370-371*, 355–367. [CrossRef]
202. Jena, P.K.; Ghosh, S.; Koley, E.; Mohanta, D.K.; Kamwa, I. Design of AC state estimation based cyber-physical attack for disrupting electricity market operation under limited sensor information. *Electr. Power Syst. Res.* **2022**, *205*, 107732. [CrossRef]
203. Li, Y.; Tao, Q.; Gong, Y. Digital twin simulation for integration of blockchain and internet of things for optimal smart management of PV-based connected microgrids. *Sol. Energy* **2023**, *251*, 306–314. [CrossRef]
204. Gao, X.; Yang, X.; Meng, L.; Wang, S. Fast economic dispatch with false data injection attack in electricity-gas cyber–physical system: A data-driven approach. *ISA Trans.* **2023**, *137*, 13–22. [CrossRef]
205. Fang, Y.; Wang, C.; Fang, Z.; Huang, C. LMTracker: Lateral movement path detection based on heterogeneous graph embedding. *Neurocomputing* **2022**, *474*, 37–47. [CrossRef]
206. Poudel, S.; Ni, Z.; Malla, N. Real-time cyber physical system testbed for power system security and control. *Int. J. Electr. Power Energy Syst.* **2017**, *90*, 124–133. [CrossRef]
207. Gawusu, S.; Zhang, X.; Ahmed, A.; Jamatutu, S.A.; Miensah, E.D.; Amadu, A.A.; Osei, F.A.J. Renewable energy sources from the perspective of blockchain integration: From theory to application. *Sustain. Energy Technol. Assess.* **2022**, *52*, 102108. [CrossRef]
208. Moshtagh, S.; Rahmani, M. Robust hybrid state estimation for power systems utilizing Phasor measurements units. *Electr. Power Syst. Res.* **2021**, *196*, 107195. [CrossRef]
209. Javed, M.A.; Muram, F.U.; Punnekkat, S.; Hansson, H. Safe and secure platooning of Automated Guided Vehicles in Industry 4.0. *J. Syst. Archit.* **2021**, *121*, 102309. [CrossRef]
210. Jansen, C. Stabilizing the Industrial System: Managed Security Services' Contribution to Cyber-Peace. *IFAC-PapersOnLine* **2017**, *50*, 5155–5160. [CrossRef]
211. Martín-Lopo, M.M.; Boal, J.; Sánchez-Miralles, Á. Transitioning from a meta-simulator to electrical applications: An architecture. *Simul. Model. Pract. Theory* **2019**, *94*, 177–198. [CrossRef]
212. Jena, P.K.; Ghosh, S.; Koley, E. Design of a coordinated cyber-physical attack in IoT based smart grid under limited intruder accessibility. *Int. J. Crit. Infrastruct. Prot.* **2021**, *35*, 100484. [CrossRef]
213. Su, Q.; Li, S.; Gao, Y.; Huang, X.; Li, J. Observer-based detection and reconstruction of dynamic load altering attack in smart grid. *J. Frankl. Inst.* **2021**, *358*, 4013–4027. [CrossRef]

214. Sethi, T.S.; Kantardzic, M. On the reliable detection of concept drift from streaming unlabeled data. *Expert Syst. Appl.* **2017**, *82*, 77–99. [CrossRef]
215. Staggs, J.; Ferlemann, D.; Shenoi, S. Wind farm security: Attack surface, targets, scenarios and mitigation. *Int. J. Crit. Infrastruct. Prot.* **2017**, *17*, 3–14. [CrossRef]