energies

MDPI

Article

Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions

Jianguo Ding [1,*], Attia Qammar [2], Zhimin Zhang [2], Ahmad Karim [3] and Huansheng Ning [2]

[1] Department of Computer Science, Blekinge Institute of Technology, 37179 Karlskrona, Sweden
[2] School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China
[3] Department of Information Technology, Bahauddin Zakariya University, Multan 60000, Pakistan
* Correspondence: jianguo.ding@bth.se

Abstract: Smart Grids (SGs) are governed by advanced computing, control technologies, and networking infrastructure. However, compromised cybersecurity of the smart grid not only affects the security of existing energy systems but also directly impacts national security. The increasing number of cyberattacks against the smart grid urgently necessitates more robust security protection technologies to maintain the security of the grid system and its operations. The purpose of this review paper is to provide a thorough understanding of the incumbent cyberattacks' influence on the entire smart grid ecosystem. In this paper, we review the various threats in the smart grid, which have two core domains: the intrinsic vulnerability of the system and the external cyberattacks. Similarly, we analyze the vulnerabilities of all components of the smart grid (hardware, software, and data communication), data management, services and applications, running environment, and evolving and complex smart grids. A structured smart grid architecture and global smart grid cyberattacks with their impact from 2010 to July 2022 are presented. Then, we investigated the the thematic taxonomy of cyberattacks on smart grids to highlight the attack strategies, consequences, and related studies analyzed. In addition, potential cybersecurity solutions to smart grids are explained in the context of the implementation of blockchain and Artificial Intelligence (AI) techniques. Finally, technical future directions based on the analysis are provided against cyberattacks on SGs.

Keywords: smart grids; cybersecurity; vulnerabilities; cyberattacks; blockchain; artificial intelligence

Citation: Ding, J.; Qammar, A.; Zhang, Z.; Karim, A.; Ning, H. Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions. *Energies* **2022**, *15*, 6799. https://doi.org/10.3390/en15186799

Academic Editors: Basile L. Agba, Marthe Kassouf and Mourad Debbabi

Received: 16 August 2022
Accepted: 9 September 2022
Published: 17 September 2022

1. Introduction

Smart grid technology has been introduced to enhance the existing electricity systems with modernization. There are various energy management and operations techniques induced in smart grid technologies in order to obtain their peak benefits. These management and operations techniques include the deployment of smart meters and applications at consumers' premises, whereas smart inverters, a production-grade meter, generators to produce renewable energy, and various energy-efficient resources are installed at the grid center. According to [1], the market size for global substation automation was predicted to be USD 39.9 billion in 2021. If it expands at the same pace, the estimated size will rise to USD 54.2 billion by the end of 2026. This growth contributes to various prominent factors, including development projects related to power grid technologies, since the electricity is produced from renewable resources ultimately contributes to cheap costs for renewable energy generators. In order to meet the growing electricity demands, new green energy sources such as hydropower, geothermal heat, wind, solar radiation, fuel cell, bioenergy, ocean energy, and nuclear fission are attached to existing electricity distribution structures [2]. Although renewable energy is embedded in nature, it is still impacted by various conditions including humidity, wind speed and direction, ambient temperature, and geographical area. For example, solar energy is affected by cloud cover, ambient temperature, and irradiance. Similarly, hydropower generation is affected by climate change, i.e., change

in rainfall pattern, flooding, intense rain, air temperature, and others [3]. In the context of smart grids, the major components are presented in Figure 1.

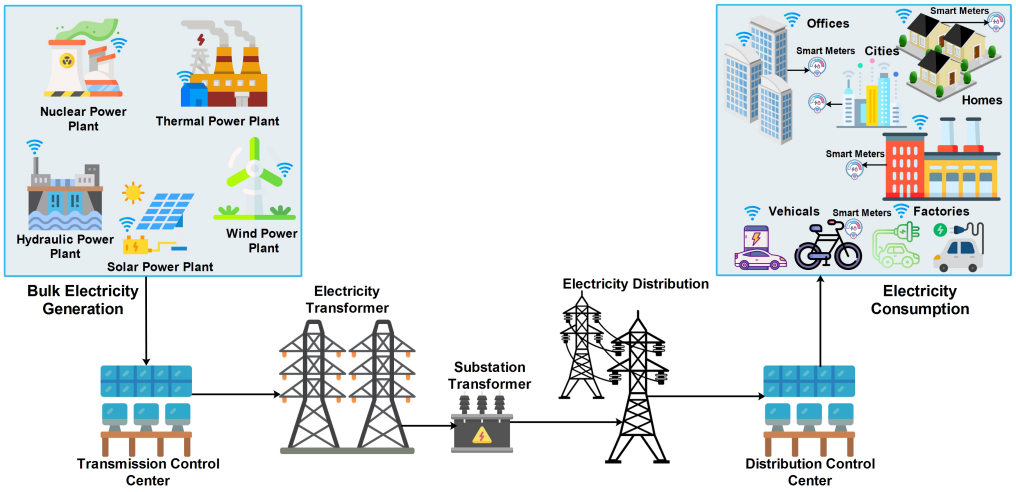

Figure 1. Characteristics of smart grid.

The overall communication network of the smart grid connects with three major components, i.e., grid, service provider, and customers. Moreover, the communication among those components governs based on different channels and protocols. Large-scaled energy generation, energy distribution, and energy transmission take place at the grid domain level. Similarly, the emergence of new energy sources, smart meters, sensors, and control devices in the smart grid enable advantages in the latest ecosystem. Advanced Metering Infrastructure (AMI) is a combined network that connects consumer premises and the communication network simultaneously. Smart meters are used to propagate usage history, outages, and consumed amounts to the cloud providers. The communication technologies that are used to communicate with the consumer domain are categorized into two types: wireless and wired. In terms of wired communication, this includes the Power Line Communication (PLC), fiber optical and ethernet, whereas wireless communication consists of cellular, WiMAX, Zigbee, Z-wave, satellite, and free space optical [4]. Additionally, the smart grid comprises various components; for example, for transmission purposes, it relies on energy management systems (EMS), and distributing the power is dependent on distribution management systems (DMS). Furthermore, the whole transmission network is examined and controlled through supervisory control and data acquisition (SCADA) system. The smart grid technologies provide various benefits over the traditional grids which includes the categories of management, control, and operation. These and many more benefits make the smart grid a more attractive choice in comparison with traditional grid systems as presented in Figure 2.

Although smart grids enable the efficient distribution of consumer consumption metrics as compared to traditional power systems, they are however prone to security attacks at various tiers [5]. Indeed, technological advancements have impacted positively on the power industry, however these advancements have also opened pathways for attackers to exploit vulnerabilities and introduced additional threats in crucial situations such as natural disasters, terrorism, and theft. Cyberattacks on smart grid security include the breaching of sensitive customer data by adversaries, malware propagation, malfunctions in cyber systems, and vulnerabilities in distributed control devices [6]. Furthermore, compromising communication equipment, injecting false information, eavesdropping, attacks on SCADA, modifications and many other attacks affect the cyber security of the smart grid. In order to mitigate and address these cyber-spaced malicious efforts, the US National Institute of Standards and Technology (NIST) proposed a framework by following the guidelines for smart grid cybersecurity issued by executive order 1363. This guideline

is specifically built to develop different pathways to minimize cyber-attacks to the critical infrastructure of smart grids [7].

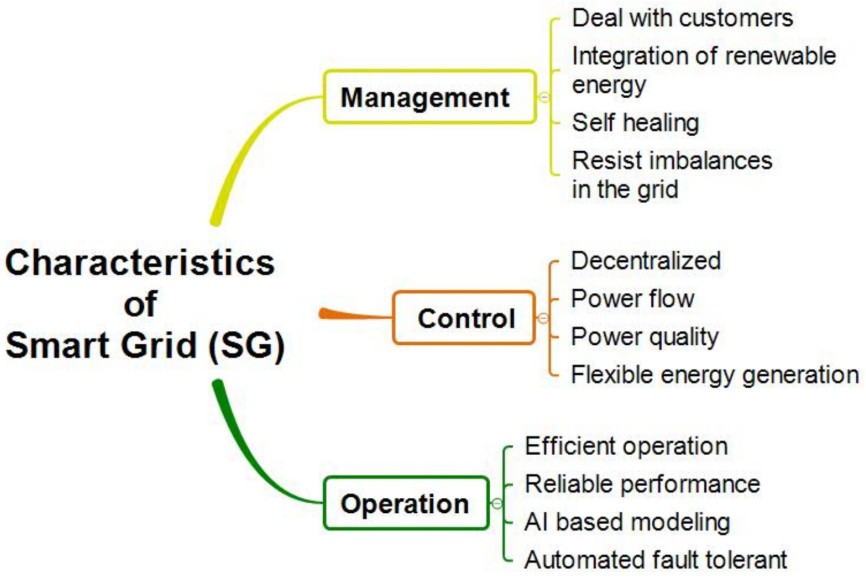

Figure 2. Characteristics of smart grid.

Vulnerabilities disturb the smart grids comprises of (SCADA), Phasor Measurement Unit (PMU), and Remote terminal units (RTU), etc. Any disruptions in electricity production jeopardized the smart grid reliability and have far-reaching socio-economic consequences. Furthermore, because valuable data are exchanged between smart grid systems, burglary or variation of these data may infringe consumer privacy. The major vulnerabilities of smart grids particularly include the lack of a firewall, misconfiguration, lack of security audits, insufficient security measures, and improper authentication, which leads to the entire smart grid system failure. Because of these flaws, the smart grid became a predominant target for attackers, attracting the attention of government, manufacturers, and academic institutions [8–10]. Cyberattacks are launched successfully when existing smart grid system have vulnerabilities, including a lack of updated security patches for software, keylogging, tampering, command injection, path traversal, and many others. Cyber security techniques are required in order to mitigate security risks and minimize cyber threats for smart grid systems. Thus, critical investigation for potential cybersecurity risks with their targets to smart grid security are required.

1.1. Overview of Smart Grid Infrastructure

A smart grid is an intelligent transformation of the traditional physical grid. Relying on advanced sensing, communication, and decision-making technology to achieve safe, efficient, and environmentally friendly transmission and power demand is the goal of the smart grid. Although the smart grid has entered the commercial stage, different countries, organizations, and institutions have given inconsistent explanations for the connotation of this term.

- SmartGrid.gov: like the Internet, the Smart Grid will consist of controls, computers, automation, and new technologies and equipment working together, but in this case, these technologies will work with the electrical grid to respond digitally to our quickly changing electric demand [11].
- National Institute of Standards and Technology (U.S. Department of Commerce): The smart grid is a planned nationwide network that uses information technology to deliver electricity efficiently, reliably, and securely. It has been called ''electricity with a brain", "the energy internet", and "the electronet". A more comprehensive definition we use at NIST is a modernized grid that enables bidirectional flows of energy and

uses two-way communication and control capabilities that will lead to an array of new functionalities and applications [12].

- Grid 2030: Grid 2030 is a fully automated power delivery network that monitors and controls every customer and node, ensuring a two-way flow of electricity and information between the power plant and the appliance, and all points in between. Its distributed intelligence, coupled with broadband communications and automated control systems, enables real-time market transactions and seamless interfaces among people, buildings, industrial plants, generation facilities, and the electric network [13].
- The Office of Electricity: An automated, widely distributed energy delivery network, the Smart Grid will be characterized by a two-way flow of electricity and information and be capable of monitoring everything from power plants to customer preferences to individual appliances. It incorporates into the grid the benefits of distributed computing and communications to deliver real-time information and enable the near-instantaneous balance of supply and demand at the device level [14].

Although these explanations are different, it is found that the smart grid usually contains three components, namely hardware, software, and interaction-based flow. As shown in Table 1, the hardware includes substations, transformers, meters, etc., in the traditional power grid, as well as sensors, automatic controllers, etc., for intelligent interaction, which are physical components in the smart grid. The software is used in the power grid hardware to realize the functions of intelligent dispatching, intelligent defense, intelligent energy storage, and so on. Networked software also plays an important role in the construction of the smart grid to realize timely and effective interaction to provide better service. Their application makes the grid no longer a closed system, but a combination of factors to achieve smarter generation, transmission, and use of electricity. Interaction-based flows mainly include electrical energy, data generated by hardware and software, and various networks for data exchange. According to the purpose of flow, they can be divided into power flow, data flow, control flow, information flow, etc. They can flow between various components of the power supply system, providing more intelligent and refined services between the power supply department and users than the traditional power grid.

Table 1. Main hardware used to build smart grids.

Power Application Stage	Related Hardware
Production	Traditional: generators, utility boilers, gas turbines, steam turbines, water turbines, etc. Intelligent: remote control module, cloud service control module, unit adjustment module, field equipment management module, etc.
Transmission	Traditional: boosters, substations, grids, high voltage switches, voltage transformers, arresters, etc. Intelligent: status monitoring device of substation equipment, airborne inspection components, etc.
Distribution	Traditional: distribution transformers, incoming cabinets, metering cabinets, outgoing cabinets, isolation cabinets, etc. Intelligent: temperature and humidity sensor, current detector, leakage detector, etc.
Consumption	Traditional: mechanical meters, induction meters, electronic meters, etc. Intelligent: remote control module, microprocessor, operation panel, A/D converter, etc.

- Internet Technology (IT) and Operational Technology (OT): IT provides conditions for the two-way interaction and sharing of information flow in the smart grid. Due to the openness of the protocol, the information collected from different components of the power grid can be circulated conveniently. The advanced technologies such as wireless communication, satellite communication, and laser communication provide diverse and accurate information acquisition and transmission services for the smart

grid.To realize the high integration of the industrialization process and information construction, the smart grid needs the help of OT. OT and IT are two different concepts, and this difference is reflected in the operation, technology, and management of the system [15]. The core idea of OT is to effectively transform the long-term accumulated manual experience into an applicable knowledge system for computers and other equipment, and build the automatic operation and management process of the power grid [16].

- Supervisory Control and Data Acquisition (SCADA): SCADA is widely used in the power system to realize the monitoring and control of field equipment [17]. In this system, the remote terminal unit (RTU) and feeder terminal unit (FTU) provide strong support for data acquisition, control, regulation, feedback, alarm, and other operations. With the continuous development of the computer industry, SCADA began to combine new technologies such as expert systems, artificial intelligence, deep learning, and knowledge inference to improve the linkage ability of all parts of the power grid [18]. However, the growth of remote accessibility between systems has compromised the security of SCADA [19].
- Cyber-Physical Systems (CPS): Realizing the deep convergence of physical space and cyberspace is the ultimate goal of CPS. During the construction of the power grid, physical space contains a variety of infrastructure related to power systems, such as power generation equipment, substation equipment, transmission equipment, and electrical equipment. Ning et al. [20] pointed out that arithmetic logic unit (ALU) with computing function, various devices used for storage, gateways/routes used for data transmission belongs to things that appear together in cyberspace. They can transform things in traditional physical space to make them have the ability of perception, computing, and communication [21].
- Internet of Things (IoT): Using sensor network, radio frequency identification technology (RFID), intelligent embedding technology, and other means, it is possible to take the network as the carrier to build a things-centered information interaction network, that is, IoT. Compared with CPS, IoT aims to realize the ubiquitous connection between physical space and cyberspace, to realize the intelligent management of things. Since power generation, transmission, and final power consumption require the cooperation and linkage of different components in the power grid, the effective management of each component is an important measure to achieve intelligence. In the process of construction and the improvement of the smart grid, the data sharing and management mechanisms of the system also need to solved in terms of perception, transmission, and application, so that they can be realized by relying on the three layers including the sensing, network, and application layer architecture of the IoT.
- Fog/edge computing: With the development of micro miniaturization, low power consumption, intelligence, high integration, and networking of sensors, fog computing and edge computing have become important technologies that can be applied in the construction of distributed smart grids [22]. At present, the transformation of the smart grid is developing towards decentralization and distribution. Compared with the current highly centralized power system, this scheme has the advantage of, in case of failure or other accidents, being able to theoretically reduce the scope and scale of influence.
- Internet of Energy (IoE): The goal of IoE is to transform the electricity-related infrastructure of existing energy producers and suppliers, making them digital, automated, and intelligent. Such transformation is a necessary basis for building a smart grid [23]. The development of IoE relies on IoT, which can help accelerate the transformation of traditional power grids to smart grids. The purpose of IoE construction is to make energy production more environmentally friendly [24], energy utilization more efficient, energy consumption reduced, and energy cost more economical.

No matter what computer technologies are used to build a smart grid, their essence is a program composed of code. Due to the lack of strict test management and security

certification, these technologies may have loopholes and backdoors. Once these defects are exploited by attackers, they will seriously threaten the integrity of smart grid operation. Malicious attacks on the smart grid may cause power outages, affect users' normal production and life, or lead to social unrest and even international disputes. Therefore, it is very important to predict risks in advance [25], ensure the stability of smart grid operation, reduce the risk of cyberattacks, and effectively protect data privacy.

1.2. Research Method

In previous years, smart grid research attracted many scholars and the growth of publications has been exponential, as presented in Figure 3. We searched keywords such as "smart grid", "cyber threats", "cyberattacks", and "vulnerabilities" with the conjunction (AND) and disjunction (OR) operators to retrieve the exact studies. Furthermore, we have included more keywords such as blockchain, Machine Learning (ML), and Deep Learning (DL) in order to define the potential solutions against smart grid security attacks. Finally, relevant studies are included from top research databases such as IEEE, SpringerLink, ACM, ScienceDirect, and MDPI.

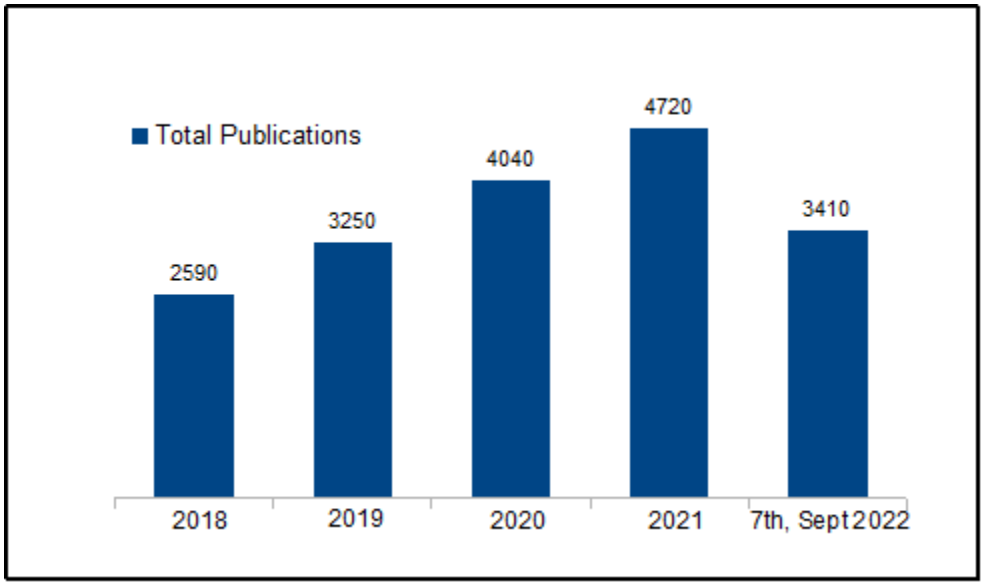

Figure 3. Year-wise publications with the search string "smart grid" AND "cyber threats" OR "cyberattacks" OR "vulnerabilities" on Google Scholar.

1.3. Our Contribution

This paper examined the smart grid threats that covered the two core domains: the intrinsic vulnerability of the system and the external cyberattacks. Furthermore, it presents the comprehensive thematic taxonomy of cyberattacks to smart grids with attack strategies and countermeasures. To detect and prevent cybersecurity attacks on the smart grid, AI- and blockchain-based techniques are elaborated. Additionally, researchers need a greater understanding of smart grid security in terms of future directions.

1.4. Organization of Paper

The remainder of this paper is organized as follows. In Section 2 we elaborated the vulnerabilities of smart grids. Section 3 described the global review of cyberattacks on smart grids. Section 4 presented the thematic taxonomy of cyberattacks on smart grids. In Section 5 potential solutions are investigated for cybersecurity in smart grids. Section 6 provides the future research directions. Finally, Section 7 concludes the paper.

2. Vulnerabilities of Smart Grids

Vulnerability is defined by CVE (Common Vulnerabilities and Exposures) as ''a weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, OR availability. Mitigation of the vulnerabilities in this context typically involves coding changes but could also include specification changes or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety)" [12].

Modern smart grids have evolved into a complex technical system that integrates physical networks, information technology (IT), and operational technology (OT), and interoperates and interacts with many other related critical infrastructures. All vulnerabilities [26] embedded in the grid system, even those of external systems interconnected with the grid system, have a direct and indirect impact on the security of the grid. Vulnerability is a major part of the threats to smart grids, and can potentially lead to various consequences, such as power outages, power losses, economic damages, etc.

2.1. Vulnerabilities in Physical Components

A smart grid consists of various components, including hardware, software, and management systems. All of these components harbor some vulnerabilities, such as:

1. Inadequate physical access control systems, e.g., inadequate camera surveillance, and inadequate surveillance at unmanned sites;
2. Inadequate physical security for DERs at remote locations;
3. Internal redundancy constraints within the substation;
4. Inadequate monitoring of long lines;
5. Obsolete components and long replacement times for damaged equipment;
6. Inadequate filtering of electromagnetic pulses near the smart grid system;
7. Poor physical environment of grid operation.

These potential risks are traditional problems that also originate from natural or man-made physical damage [27], and there are also many proven means and methods of protection. However, these physical vulnerabilities have the potential to facilitate a possible coordinated cyberattack, a combination of local and adversary cyberattacks.

2.2. Vulnerabilities in IT/OT

Information technology (IT) and operational technology (OT) networks have historically operated independently. Electric utilities have relied on IT to automate business functions such as daily management, billing, customer service, and accounting, while OT has focused primarily on managing electric grid operations such as power distribution, and critical energy infrastructure management. Advances in IT/OT have led to the ability of connected substations that can work together with little or no human interaction. As more and more smart devices are integrated into smart grids, it is becoming increasingly challenging to keep the grid secure. This connectivity between IT and OT is changing the philosophy and approach to the cybersecurity of smart grids. However, at the same time all the vulnerabilities that IT/OT possesses become a threat component to the overall grid system.

1. Vulnerabilities in Hardware and Software
   Smart grids consist of a large number of different smart hardware and software, especially networked devices. Any vulnerability in this hardware and software can lead to corresponding cyberattacks [28]. These devices include:
   - Field devices I/O, such as pump, sensor, fan, valve;
   - Control level, such as HMI, RTU;
   - Process level, such as HMI, SCADA server;
   - Operation workstation, various servers, such as DNS servers, file servers, mail servers;
   - Network devices, such as routers, IT&OT DMZ;

- Enterprise IT, such as ERP, Mail, CRM, security operation center (log Management, SIEM, Analytics).

The reported vulnerabilities in National Vulnerability Database (NVD), Vulnerability Database (VULDB) [29], and CVE Details [30] demonstrate the increasing vulnerabilities in the hardware/software of smart grid and general software [31]. The CVE and CVSS show the long-term trend of increasing vulnerabilities on smart grid devices and combined software [30,32]. The vulnerability of these smart grid devices with intelligent operation and networking capabilities is growing rapidly, not only because of more vulnerabilities in the new devices but because of evolving smart grid systems, newer smart grid operating environments, and expanding applications and services.

2. Vulnerabilities in data communications
Various modern communication technologies are used in different areas of the smart grid, such as IEC 61850, IEC 60870-5-104, DNP3, PRP/HSR, Modbus, Synchrophasor, DLMS/COSEM, AMI, TASE.2/ICCP, NTP, and also the protocols used in IT parts, as well as other new communication technologies and protocols. These communication technologies and protocols themselves contain various traditional and new vulnerabilities [33]. These vulnerabilities also facilitate various communication and network-based attacks [26,34].

The communication in the OT part lacks sufficient security design to protect the data communication within OT components and with the IT components. This is primarily a weakness of smart grids that is hard to fix in the short term. Replacing technologies and devices and improving OT can take quite a long time. The vulnerability in IT communication is not new, but it is a channel that connects the external attacker with the internal OT.

2.3. Vulnerabilities in Data Management

Current smart grid data management faces the problem of data aggregation quality, security, compliance control, common scope, and efficiency of the management mechanism. A large amount of data is generated and transferred between different entities. Accurate and consistent incoming data streams such as grid operation, weather forecasts, and business data allow operators to control and monitor the grid system. Such information is very important to avoid sudden and unexpected power supply disruptions and to maintain the quality of grid services and business. In addition, such big data can also be used for grid operations, alarms, demand forecasts, generation estimates, price adjustments, etc. The data collected tend to be quite large, as multiple smart grid domains are involved in the process. There is also a regulatory requirement to provide accurate data as frequently as possible, which is challenging. However, there are many vulnerabilities in the long chain of data collection, analysis, processing, maintenance, and security in the cyber environment. Most smart grids are not prepared to maintain data security and privacy management. The vulnerability is demonstrated by the inadequate CIA triad (confidentiality, integrity, and availability) for data and the protection of services [5,8] and the lack of specific protection technology for smart grid domain data, such as generated data from the field device data, SCADA, grid operational data, and transaction data, etc.

2.4. Vulnerabilities in Services and Applications

Access to OT data and IT data enables the rapid transformation of physical data into actionable information that enables advanced asset management platforms, distributed energy management systems, and distribution grid applications. The applications have led to some amazing benefits for asset-rich substations. Inter-connectivity leads to faster data exchange between devices, enabling automation of substation protection and control systems and providing operational benefits. Smart grids can provide quite a number of applications and services for electricity trading, electricity services, electricity convergence, and various customer services. All these digitization-based services rely on grid operation, grid communication, data collection, and application process analysis.

Smart grid services and applications include the following areas: (1) AMI-based applications and services (e.g., demand-side management, home energy management); (2) distributed generation management (i.e., DER management); (3) advanced distribution/transmission automation (e.g., substation automation, storage management, advanced distribution applications, islanding solutions, etc.); (4) client services, and added-value services built upon them.

There are some inherent vulnerabilities in information technology system applications, which are greatly expanded in scale on the smart grid and extend to all aspects of applications and services [35,36], which include:

1. Lack of patching policy and regular updates, e.g., unpatched software and systems;
2. Common mode failures;
3. Improper asset management;
4. Improper maintenance documentation;
5. Use of outdated operating system versions;
6. Inadequate AAA: authentication (to identify), authorization (to grant permission), and accounting (to log an audit trail);
7. Poor grid isolation from the Internet;
8. Lack of intrusion detection systems for OT;
9. Inadequate malware detection and defense for OT;
10. Unreliable technology provider for those OT devices;
11. Inadequate compatibility with legacy systems and legacy devices.

All these vulnerabilities seriously disrupt the regular functions and services of smart grids.

2.5. Vulnerabilities in Running Environment

The smart grid operating environment includes many levels, from technology to society, people, ethics, politics, national policy, and the international environment [35,37]. Therefore, the typical vulnerabilities for the grid operating environment include many non-IT aspects, such as:

1. Staff incompetence, e.g., lack of professional skills, unreliable and dishonest behavior, etc.;
2. Weak controls on legal, social, and ethical aspects;
3. Weak relationships between managers;
4. Inadequately controlled outsourcing;
5. Non-compliance with national and international regulations;
6. Political, war, or regional conflicts;
7. Terrorism;
8. Government corruption;
9. Pandemics.

Most of the above vulnerabilities should be addressed with both technical and non-technical solutions, such as improving cybersecurity awareness, sufficient professional training, and continuous monitoring of the entire operating environment of the smart grid. Since the smart grid is a typical critical infrastructure, the system could be more targeted by attackers in troubled environments. Therefore, the political and international background should not be ignored.

2.6. Vulnerabilities in Evolving and Complex Smart Grids

The expanding and evolving smart grids are integrating more and more IEDs (Intelligent Electronic Devices) and components, bridging to different network systems, supporting more and more applications and services, and interacting with other critical infrastructures. This makes smart grids a typical SoS (system of systems). Any vulnerability in any part of the complex systems puts the smart grid at risk, and the dynamics and complexity make vulnerability detection and remediation even more challenging [38,39].

The vulnerability identification, detection, and remediation should be managed systematically and need to combine with the cyberattack analysis. Most of the cyberattacks make use of the vulnerabilities in a smart grid system, in particular the vulnerability in those networked devices and components.

Smart grid security is not just about building networks that are defensible (i.e., can withstand any threat). A more logical approach is to have an efficient network vulnerability management, that can adapt quickly to changing conditions while minimizing damage to smart grids. The main tasks for vulnerability management are as follows:

1. Identify and detect as many and as complete vulnerabilities as possible at all levels of the system, as any undiscovered vulnerability can lead to potential security risks. The security of the smart grid is determined by the weakest part, not by the strongest part.
2. Repair or remove system vulnerabilities as soon as possible. Once vulnerabilities exist and are discovered, hidden threats must be eliminated as quickly as possible. Many cyberattacks exploit zero-day vulnerabilities.
3. Vulnerability aggregation. The final vulnerability of the system is not simply a collection of vulnerabilities. It is necessary to clarify the physical, logical, and functional dependencies between them and figure out their aggregation rules. This enables a complete understanding of the system vulnerability of smart grids.
4. Automated discovery and analysis of system vulnerabilities are necessary. The smart grid system contains various vulnerabilities, and it is difficult to find all vulnerabilities manually with exhaustive methods and analyze them in time. Automated methods need to be developed to support vulnerability detection, analysis, and management.
5. Vulnerability analysis and attack matching. All cyberattacks exploit one or more vulnerabilities in a system. A clear map of vulnerabilities and attacks is very helpful in defending and protecting system security.
6. It is necessary to create a systematic plan with countermeasures to address the vulnerabilities. A single point of failure or weak point of failure is always a challenge to a smart grid.

3. Global Review of Cyberattacks to Smart Grids

Due to the high dependence of the smart grid on computer networks and other related technologies, cyberattacks will interfere with the normal operation of power systems. In addition, power production, transmission, and application are closely related to the industry, agriculture, medical treatment, and other aspects. Once the power grid is attacked, it will cause immeasurable losses to normal production and life. Table 2, summarizes the serious smart grid attack and destruction events worldwide between 2010 and July 2022 and briefly describes the impact and consequences of the events.

Summarizing the above attacks against smart grids, it is found that the reasons for these losses mainly include two aspects, namely, the vulnerability of the smart grid and cyberattacks launched by exploiting vulnerabilities. Unreasonable smart grid structure, no safety-certified application software, and untimely maintenance of software and hardware may leave potential safety hazards for the normal operation of the smart grid. The construction, use, and maintenance of these smart grids may also not strictly adhere to the five aspects of cybersecurity risk management, namely identify, protect, detect, respond, and recover. Once these vulnerabilities are discovered by attackers and used illegally, the power system may suffer severe damage. Currently, cyberattacks launched by exploiting smart grid vulnerabilities mainly use ransomware and malware.

By encrypting sensitive data of the power sector, users, and even partners, the attacker achieves the purpose of extorting the power company. Except for ransomware developers, the power sector has almost no ability to decrypt these files. For general computer systems, ransomware mainly achieves intrusion through vulnerabilities, emails, and unsafe links to web pages.

Table 2. Globally serious smart grid attacks and damages.

Time	Location	Attack Target(s)	Attack Method(s)	Attack Range	Impact and Consequence	Reference
2010	Iran	Disrupt the nuclear centrifuges	Stuxnet virus	-	Nearly one-fifth of Iran's nuclear centrifuges were destroyed. The worm infected over 200,000 computers and damaged 1000 devices by targeting industrial control systems.	[40,41]
September 2011	Arizona, Southern California	affected nearly 2.7 million customers	-	-	This problem causes huge variance between the demand and power supply resulted in a noticeable frequency drop, tripping, and blackout.	[42]
December 2014	Korea	goal	Malicious Code "kimsuky"	Korea Hydro and Nuclear Power plant	Sent 5986 phishing emails containing malicious codes to 3571 employees of the nuclear plant operator.	[43]
December 2015	Part of Kiev (the capital of Ukraine) and western Ukraine	Transformer substations	BlackEnergy malware	30 seats	About 1.4 million residents had power outages in their homes, disrupting phone calls from power companies that prevented residents from contracting them properly.	[44]
January 2016	Israel	National power supply system	Malware	-	The government had to suspend the operation of a large number of computers in Israel's power facilities.	[45]
June 2017	Ukraine	Chernobyl nuclear power plant	Petya blackmail virus	Unknown	Several national power facilities were infected, resulting in abnormal operations.	[46,47]
June 2018	France	French company Ingerop	Malicious software	Sensitive data of Fessenheim nuclear power plant	Hackers stole more than 65 GB of sensitive data. These data included nuclear power plant plans and the personal information of thousands of staff.	[48]
March 2019	United States (U.S.)	U.S. power grid	Denial of service (DoS) attack	The Western U.S.	The accident did not cause power failure, and the machine failure time was less than 5 min.	[49]
August 2019	South Africa (Johan-nesburg)	City Power company	Blackmail software	All databases, applications, web apps, and official websites of the company	The attack prevented users from buying electricity, recharging, processing invoices, and accessing the official website of City Power.	[50]
August 2019	Ukraine (Yuzh-noukrainsk)	NPP	Intranet connection to extranet	All sensitive data inside the nuclear power plant	The accident was classified as leakage of state secrets.	[51]
April 2020	Portugal	Energias de Portugal	Blackmail software (Ragnar Locker)	Confidential information within the company	The attacker claimed to have acquired 10TB of sensitive data, including bills, contracts, transactions, customer, and partner sensitive contents.	[52,53]
June 2020	Europe	Enel Group	Snake blackmail software	Internal IT network	The internal IT network was temporarily blocked, resulting in a temporary interruption of customer service activities.	[54]

Table 2. *Cont.*

Time	Location	Attack Target(s)	Attack Way(s)	Attack Range	Impact and Consequence	Reference
June 2020	Brazil	Light S.A (Power company)	Sodinokibi blackmail software	Confidential information within the company	The attacker extorted USD 14 million in ransom, and only the attacker's private key could decrypt the file.	[52]
September 2020	Palestine	K-Electric (Power supplier)	Netwalker blackmail software	Unencrypted files	An unknown amount of stolen data, power billing, and online service interruption.	[55]
February 2021	Texas	-	-	Texas energy market failures	February's "Big Freeze" winter storm vulnerable to Texas energy market failures.	[56]
April 2022	Ukrainian	Energy company	Industroyer2 malware	-	Industroyer2 directly connects with electrical utility equipment to send commands to the substation devices that regulate the flow of electricity.	[57]

For the local area network of the electric power department that stores a large amount of sensitive data, the probability of ransomware intrusion through vulnerabilities is far greater than that of emails and unsafe links. In addition to demanding a huge ransom from the power company, ransomware may also cause interruption of normal user services and even serious consequences of not being able to supply electricity.

As national infrastructures, the power grid has become an important target for network confrontations between countries and hacker sabotage. Therefore, malware targeting the smart grid is also constantly evolving. Under the premise of being as concealed as possible, this malware is dedicated to increasing the intensity and scope of damage to the grid. Some malware can run in the power grid control system in a hidden way. By interfering with the power distribution function of the system, it causes uneven power distribution, wastes power resources, and reduces energy utilization. In addition, malware can cause the substation to lose the connection with the control center to achieve the purpose of cutting power transmission, which may cause paralysis of production, transportation, and medical care. A more serious situation is that if malware invades nuclear power plants and control key functions such as operating nuclear reactors, there may be casualties and even social conflicts.

4. Thematic Taxonomy of Cyberattacks to Smart Grid

The exploration of cyberattacks on smart grids has so far predominantly relied on false data injection attacks (FDIAs), denial of service (DoS) attack, data framing attacks (DFA), man-in-the-middle (MiTM) attack, load altering attacks (LAAs), false command injection attack (FCIA), load redistribution attack (LRA), coordinated cyber–physical topology (CCPT) attacks, replay attack, etc., as presented in Figure 4. These diverse kinds of cyberattacks accentuate and exploit different vulnerabilities in power grids with different attack intents and strategies. Furthermore, deep integration of information systems into power physical systems leads to severe threats such as malware attacks and so on.

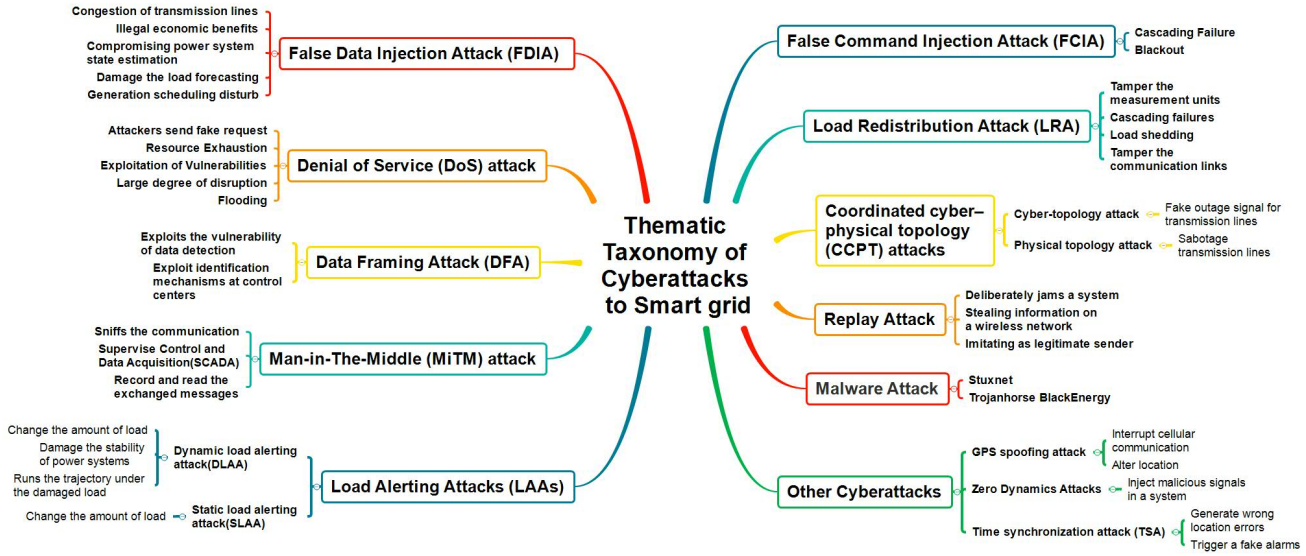

Figure 4. Thematic taxonomy of cyberattacks to smart grids.

4.1. False Data Injection Attack

False data injection attacks (FDIAs) were first developed in [58], aiming to masterly interfere with the meter measurements and invisibly influence the result of state estimation (SE), posing a serious threat to smart grid security. Furthermore, FDIAs are capable of evading the bad data detection (BDD) mechanism of the smart grid. In the past decade, FDIAs on smart grid systems received noticeable attention due to their influences. With the tremendous proliferation of cyber–physical systems, FDIAs are broadly gaining illegal profit by tampering with data and destroying the stability of electric power grids [59]. The SCADA system employed the state estimation to measure data and utilized estimated states, i.e., phase angle and bus voltage for stability analysis of transmission as well load shedding. Moreover, at the control center, an energy management system (EMS) is implemented to determine that the smart grid operating normally in terms of results on state estimation. Ultimately, the correctness of state estimation affects the working and stability of smart grids. As a result, state estimation is critical to the consistent control and operation of smart grids.

Nevertheless, state estimation is susceptible to a variety of cyber–physical attacks, the most challenging of which are false data injection attacks (FDIAs). FDIAs are skilled in fudging network topology in order to deceive the control center, disrupt the electricity market to gain revenue, and cause havoc in power grid applications such as the SCADA system and the phasor measurement unit (PMU). The implications of FDIAs on smart grids have been studied in a number of publications, including [60–62]. In the work of [60], authors investigated that FDIAs can successfully launch the branch outage sequence which disrupts the various branches concurrently and ultimately fallouts in sequential outages. Similarly, Liu et al. [61], investigated that FDIAs were able to disguise the line outage through troublesome PMU data-dependent outage detection. Furthermore, Tan et al. [62], elaborated that FDIAs lead to smart grid frequency expedition, blackouts, and damage the electric equipment. Consequently, various detection methods are developed against FDIAs detection such as deep learning, Kullback–Leibler distance, sparse optimization, colored Gaussian noise, spatio-temporal correlations, Kalman filter, and blockchain are presented in Table 3.

Table 3. Methods and countermeasures to defend against FDIA.

Reference	Key Method	Explanation
[63,64]	Deep learning	Authors proposed the deep-learning-based locational detection (DLLD) framework to detect the location of FDIAs in real time. The DLLD framework is combined with regular bad data detector (BDD) and convolutional neural network (CNN) to eliminate low-quality data and to record the inconsistency in electricity flow due to FDIAs, respectively. Similarly, a false data detector (FDD) concatenates with CNN to detect fake information and co-occurrence dependency of electric flow. From both research and experimental results, this method performs efficiently under attack conditions.
[65]	Kullback–Leibler distance	A joint transformation scheme is implemented to detect the FDIAs in real time. The presented method is assembled on the dynamics of measurement variations. Furthermore, Kullback–Leibler distance is used to determine the variance between probability distributions resulting from measurement variations. For validation purpose, the method is evaluated by IEEE 14-bus system under attack and provided great detection probability.
[66]	Sparse matrix separation	In sparse matrix separation, in-depth analysis is performed based on the attack properties to detect FDIAs, as it can block the transmission lines and infringes financial benefits with stealth. Through the sparse matrix mechanism, the compromised matrix and normal measurement matrix are detected and recovered from the corrupted measurement matrix.
[67]	Colored Gaussian noise	With the implementation of colored Gaussian noise, the detection of FDIAs is made possible and tested on independent component analysis (ICA), which relates to the unobservable FDIAs scheme. Furthermore, the performance of the attack detector is evaluated on the IEEE 30-bus power system, benchmarked to traditional Gaussian noise detector.
[68]	Spatio-temporal correlations	A Spatio-temporal detection method is to detect and evaluate the false data injection attacks. The temporal and spatial correlation are examined through cubature Kalman filter and Gaussian process regression, respectively. Both are applied to record the dynamic properties of state vector. After that, deep CNN is trained to investigate the system is under FDIAs or not. Consequently, performance shows 99.84%-100% accuracy.
[69]	Kalman filter	With the combination of Kalman filter and recurrent neural network (KFRNN), an effective scheme is presented to detect FDIAs in smart grid. At the first stage, Kalman filter and RNN are applied for state prediction to fit linear and nonlinear data features, respectively. The second stage used the fully connected layer and back propagation (BP) to adaptively concatenate the outcomes of two base learners. Moreover, dynamic threshold is measured to identify the occurrence of FDIAs with the fitting Weibull distribution of the sum of square errors (SSEs) within the observed and the predicted measurements.
[70]	Blockchain	As information is switched between independent system operation (ISO) and under-operating agents, an FDIA is generated to check the security level. Attack results in loss of network stability and economic loss to the operator. For this purpose, a blockchain-based secure architecture is developed to switch data between ISO and under-operating agents. Finally, the achieved results prove the effectiveness of blockchain in order to improve the social welfare for power system users.

4.2. Denial-of-Service Attack

Smart grid cybersecurity conforms to the availability to access power, associated information, and communication structures. In this context, a cyberattack denial-of-service (DoS) targets the availability of power and compromises reliable access in a timely manner to the smart grids [71,72]. It is prevalent because, despite its simplicity, an effective DoS attack can induce significant disruption. A DoS attack consists of either (1) flooding to overwhelm the device or channel with data, (2) manipulation of vulnerabilities or anomalies in protocols and systems or (3) both. Moreover, DoS attacks are generated through a number of dispersed individuals such as a botnet known as distributed denial-of-service (DDoS). However, the smart grid definition relates to guaranteeing access to enough power. Hence, a DoS attack on the smart grid attacks the availability of traditional use of power, denies control of communication, computing, and information systems, compromises the data integrity, and includes the denial of power itself. Consequently, any of these DoS attacks in the Smart Grid domain can result in a trickling blackout, leaving thousands, if not millions, of consumers without electricity for extended periods of time [73]. DoS attacks disrupt internet traffic and have formally cost billions of dollars around the world. With the proliferation of networking of smart grid system, DoS attacks cause major

power breakouts and lead to quite harmful consequences. In smart grids, there is a set of measurement devices including smart meters, smart appliances, data aggregators, a phasor measurement unit (PMU), a remote terminal unit (RTU), intelligent electronic devices (IEDs), programmable logic controllers (PLCs), etc. On these devices, various vulnerabilities are exposed to attack the DoS as the adoption of internet standard protocols. Furthermore, security in smart grids is overlaid which leads to numerous flaws in cybersecurity. For instance, numerous utility companies do not reportedly categorize the PMU networks as critical cyber assets, which may contribute to a structural and underlying lack of competence against cyberattacks, particularly DoS variants [74]. Similarly, the impact of a DoS attack can range from minor to severe, jeopardizing the service's availability and integrity. Moreover, this causes power line failures as well as financial loss [75]. Consequently, various detection methods are developed against DoS attack detection such as the deployment of honeypots, machine learning, data-driven software-defined networking (SDN) deep learning, and Blockchain, which are presented in Table 4.

Table 4. Methods and countermeasures to defend against DoS Attacks.

Reference	Key Method	Explanation
[75]	Deployment of honeypots	Honeypots are specially formulated devices that imitate the intended target of malicious attacks. The deployment of honeypots is suggested as a part of smart grid systems. Moreover, honeypots are implemented to detect, deflect, and analyze attacks. As advanced metering infrastructure (AMI) is an important component of smart grid, vulnerable to DoS attack. Authors presented the honeypots as decoy system in AMI to collect the attack details. The interaction between attacker and defender are investigated with optimum schemes at both sides.
[76]	Machine Learning	Machine learning (ML) based models in smart grid are used to detect DoS attacks. ML algorithms are principally used to identify DoS attacks or abnormal behavior. In first phase, it collects network data. Secondly, it selects features and employs principal component analysis (PCA). Finally, an ML algorithm is implemented.
[77]	Data-driven	The dynamic states of components subjected to DoS attacks are predicted using a data-driven scheme based on relationships between the state of the attacked modules and the rest of the components of a system before the DoS attack. It is possible to determine the time-series data for PMUs under DoS attack using interrelations among the PMU time-series, even when the attack size is quite large.
[78]	Software defined Networking (SDN)	A software-defined networking (SDN) approach is implemented with light-weight entropy-based method to detect low rate and high-rate DDoS attack. Through the adaptive threshold scheme, the highest detection rate is achieved.
[79]	Deep Learning and Blockchain	In order to achieve consensus in energy network a practical Byzantine fault tolerance (PBFT) algorithm is employed within blockchain framework. Furthermore, to detect DDoS TCP (transmission control protocol) and DDoS UDP (user datagram protocol) attack, a deep learning algorithm recurrent neural network (RNN) is implemented.
[80]	Intrusion Detection and Prevention System (IDPS)	IDPS guarantees confidentiality, integrity and availability (CIA). IDS aims to analyze the security events and identify malicious activities. In smart grids, IDPS can be applied on entire SG or AMI, SCADA, subsation and synchrophasor.

4.3. Data Framing Attacks

Smart grid security has attracted the attention of the research community towards data framing attacks (DFA). DFA has an objective to misguide the control center regarding the origin of a state attack. It was originally presented in the work of [81] as a DC model, and after that was protracted to the AC model [82]. In comparison with FDIAs, DFA does not anticipate passing the bad data detection (BDD). The malicious measurements lead to bad data which are investigated due to minor errors or malicious attacks. Furthermore, the validation process of topology and meter data is known as BDD. However, it tries to mislead the bad data identification and removal (BDIR) to separate the benign measurements from malicious data and keep them in the system which finally creates a perturbation. Furthermore, BDIR removes the benign data and provides results in inaccurate state estimation. Hence, the effective detection of data framing attacks is suggestively important

for smart grid operation and control. In the study of [83], the authors implemented machine learning (ML) to detect data framing attacks. The detection of DFA is conducted through the classification method, and classification is performed between secure data and bad data with the support vector machine (SVM) algorithm. Eventually, results are evaluated on the 118-bus IEEE test system and SVM successfully detects the data framing attack.

4.4. Man-in-the-Middle (MITM) Attack

The man-in-the-middle (MiTM) attack in the smart grid system sniffs or interrupts the communication between field devices or field devices or the Supervise Control and Data Acquisition (SCADA) system and controller. Additionally, MiTM attacks are launched to alter the information swapped at Modbus TCP communication channel. Furthermore, MiTM attackers can save as well as read the transferred messages [84]. The three main objectives of the MiTM attacks on smart grids are: (1) interrupt or reserve the measurement; (2) modify the smart meter data; and (3) alter the network traffic by an attacker [85]. In [86], the facts show that 95% of HTTPS servers are susceptible to MiTM attack, in which attackers act as a legitimate source at the destination point and are masked as the source's genuine destination. SCADA is the core component of the smart grid network that is used to deal with numerous infrastructures and plays a crucial role for electricity companies and process firms consisting of the water, gas, oil, and power sectors, etc. Some researchers [87] launched an MiTM attack on SCADA communication that utilized the International Electrotechnical Commission (IEC 60870-5-104) protocol. On the SCADA, a packet assessment technique is employed for the detection of MiTM attacks, and it relies on the address resolution protocol (ARP) poisoning approach. Additionally, security vulnerabilities in the remote terminal unit (RTU) are analyzed by generating the MiTM attack on it. As advanced metering infrastructure (AMI) in the smart grid automatically records the reading of power utilization with communication medium, it is also vulnerable to MiTM attack. Besides, Modbus transmission control protocol/internet protocol (TCP/IP) is broadly used in smart grid systems [88]. However, attacks on the Modbus TCP/IP exploit the smart grid [89]. In this context, the authors of [90] analyzed the security extortions of MiTM attack on the AMI and concentrate on the vulnerabilities in Modbus TCP/IP protocol, which is implemented through AMI for communication purposes. Consequently, various detection methods are developed against MiTM attack detection such as machine learning, physical unclonable functions (PUF) authentication, and intrusion detection system (IDS), which are presented in Table 5.

Table 5. Methods and countermeasures to defend against MiTM Attack.

Reference	Key Method	Explanation
[91]	Machine Learning	Extensive research is performed on the detection of MiTM attack in smart grid. Firstly, input observer is designed for power grid system and database with several normal and malicious features are generated. Secondly, machine learning technique is implemented on the phasor measurement unit (PMU) information. ML-based algorithms such as support vector machine (SVM) and K-nearest neighbor (KNN) are employed to classify normal and attacked classes. Furthermore, type of attack such as MiTM and DoS attacks are also recognized successfully.
[92]	PUF Authentication	A light-weight physical unclonable functions (PUF) authentication technique is used for the prevention of MiTM attack in smart grid. The proposed PUF authentication technique is applied on the smart meter and share the keys of the enrolment phase with each other. Unique keys are shared as a digital footprint with PUF scheme. Through keys, nodes are able to share information in encrypted form. Hence, the evaluated results show that the MiTM attack on smart meters is not possible in PUF authentication.
[93]	Multiple alerts from intrusion detection systems	MiTM attack lead towards the false data injection (FDI), false command injection (FCI) and replay attacks in smart grid. At earlier stage on DNP3-based MiTM attacks on a SCADA system in smart grid. Then, at the second stage, the MiTM attack is detected with IDS alarm alerts by considering the network metrics, including retransmission rate, round trip time (RTT) and processing time. It is significantly necessary to observe the network metrics to identify the signature of stealthy MiTM attack. Consequently, the effectiveness of MiTM attack is reduced.

4.5. Load Altering Attack

Load-altering attacks (LAAs) alter the power usage of targeted loads with the goal of having line overloading. LAAs have employed two techniques such as direct hacking of load and indirect load modification through exploitation. For instance, incorrect price information is broadcasted to the clients in terms of demand-side management methods. Power loads are required to manage in a cost-efficient way and protect in order to evade circuit overflow [94]. LAAs are categorized into dynamic load-altering attacks (DLAAs) and static load-altering attacks (SLAAs). Authors [95] demonstrated the DLAAs, which have the worst impact in variations of load through directing the attack load in form of a closed loop. The SLAAs comprise the erstwhile manipulation of the load, whereas in DLLAs attacker modified the amount of load as goes on to monitor a certain trajectory [96]. In comparison with SLAAs, DLAAs are more severe, the attacker needs to observe the certain electricity frequency and modify the load in reaction to the instabilities of the signal. In the market [97], frequency measuring sensor devices are available and can be deployed at any smart grid system. However, these devices are already in use to measure the sensitive frequency loads [95,98]. Due to LAAs, unexpected and sudden manipulation of power grids is increased. Further, this leads to the high operational cost of smart grids and sometimes causes unsafe frequency trips. The under the frequency load shedding (UFLS) mechanism in the smart grid is used to cope with large-scale shutdowns. However, LAAs remain efficient at damaging the power grid system in terms of partition and holding the load shedding schedule [99]. Accordingly, a few detection methods against LAAs such as observer-based, adaptive fading Kalman filter (AFKF), and model-free defense framework are discussed in Table 6.

Table 6. Methods and countermeasures to defend against LAA Attack.

Reference	Key Method	Explanation
[100]	Observer-based detection	The power system is subjected to attack under the DLAA as two vulnerable loads are proposed to examine the effectiveness of attacks on the system. After that, a robust observer mode is designed to detect load frequency with residual signal generation. Consequently, evaluation done through three generators and six buses of the power system to show the feasibility of detection.
[101]	Adaptive Fading Kalman Filter (AFKF)	In order to detect DLAA, a smart grid model is proven, then adaptive fading Kalman filter (AFKF) is established to predict the state of smart grid. Gaussian noise of the smart grid is removed through AFKF to achieve accurate state modification curve. Furthermore, Euclidean distance ratio, which is a detection algorithm, is presented based on the AFKF. Hence, amplifying the invisible DLAA by Euclidean distance ratio enhances the DLAA detection acuteness, particularly in terms of weak DLAAs.
[102]	Model-free defense framework	A unique defense strategy based on the model-free technique is presented for load frequency control (LFC) system. The defender has an objective to learn diverse LAAs and achieved learned evidence for attack attenuation as an active defense (AD). Moreover, a model-free passive defense (PD) proposed where the defender tolerates a load-altering attack through improving the system redundancies. As a result, both AD and PD techniques work effectively and are evaluated on IEEE benchmark systems.

4.6. Malicious Command Injection Attack

In power grids, the phase shifting transformers or phase shifters are utilized to control the flow of electricity. Phase shifters are implemented to prevent the congestion of electricity in transmission lines and implement the regulation on the bases of contractual compulsions. In an automated power grid system phase shift commands are transmitted through SCADA system. Accordingly, this situation is invisibly susceptible to cyberattacks. Both kinds of commands are sent from phase shift such as benign and malicious. In case of malicious commands lead to severe damage, surplus transmission lines, disconnection of power, and huge financial loss by unsettling the cross-network interchange [103]. Furthermore, SCADA can initiate malicious commands masked in the legitimate form to launch physical perturbations [104]. Additionally, [105], another related attack, tap change commands, has also been investigated in smart grids. The transformer taps are extensively utilized to

control the bus voltage in a communication network. Such attacks adversely damage the system operation and strike for fabrications. The adversary can exploit the SCADA system, modify the measurements, and hide the malicious command injection attack. Furthermore, malicious transformer taps modify the command injection attack where the transformer taps are frequently altered through on-load tap changers (OLTC) to meet a set of indicated voltages. Accordingly, a few detection methods against MCIA, such as the long short-term memory (LSTM) network-based method and the lightweight index algorithm beat bad data detection (BBDD) method are discussed in Table 7.

Table 7. Methods and countermeasures to defend against MCI Attack.

Reference	Key Method	Explanation
[106]	Long Short-Term Memory (LSTM) network-based	For the detection of malicious code from smart meters, a long short-term memory (LSTM) network-based technique is proposed on the side channel of power utilization of CPU or MCU. The evaluation done on the real-case smart meters and achieved results shows the efficiency with an accuracy of 92%.
[105]	Light-weight index Algorithm	A light-weight algorithm is proposed that has the capability to detect the occurrence of stealthy malicious tap modified commands. The algorithm is developed on the intuition bases in which attacks related to false data and commands only affect the measurement and estimation of particularly designated variables instead of all of them. The algorithm relies on the branch current to the voltages of end nodes of the tap modifying transformers.
[103]	Beat bad data detection	A detection algorithm is capable of detecting the existence of anomalous phase shifts in the response of cyberattacks. The algorithm is established on detection features and particularly includes the four indices based on branch ratio and injection currents to terminals. Moreover, reference values are counted at the phase shift selection with the evaluation of discrete indices.

4.7. Load Redistribution Attacks

The authors of [107] introduced the load redistribution (LR) attacks that relate to the state estimation-false data injection attacks (SE-FDIAs) in which the measurement of load buses and electricity flows are corrupted, whereas the demand for total power is not modified. Hence, this influence of the attack is a load redistribution (LR) through the network. Additionally, LR causes financial loss and other physical damages, i.e., tripping of lines or direct attacks on lines. For instance, LR can hack the solution of the SCED (security-constrained economic dispatch) problem in which the operator utilized the finest dispatched generator and resolve load shedding. Similarly, the two types of LR attacks are: (1) immediate LR attack, which hacks the SCED problem in order to exploit the operational cost due to load shedding; and (2) delayed LR attack, which hacks the SCED to implement the solution in terms of tripping of lines. Accordingly, detection methods against LRA such as nearest neighbor-based detection scheme, support vector model, and machine learning-based approach are elaborated in Table 8.

Table 8. Methods and countermeasures to defend against LRA Attack.

Reference	Key Method	Explanation
[108]	Nearest neighbor-based detection scheme	To detect the load redistribution attack, nearest neighbor-based detection method is proposed and scaled from a small to a large system with promising constant detection performance. A sensitive analysis as well as broad testing is conducted on the LR attack with unsystematic anomalies load changes. Furthermore, through the statistical method, the attack is localized, and the probability of each load under attack is uncovered.
[109,110]	Machine learning Based	Three types of machine learning algorithms such as nearest neighbor, support vector machines (SVM), and replicator neural networks are employed as anomalies detectors to detect cyberattacks that malevolently redistribute loads by transforming the measurements. These anomaly detection algorithms are tested with realistic historic datasets collected from PJM zonal data mapped [111]. Results presented that among the three, the nearest neighbor algorithm worked efficiently and reduced the computational cost. Similarly, LR attacks are detected via multi-output support vector regression (SVR) which worked as a load predictor and later applied the SVM.

4.8. Coordinated Cyber Physical Topology Attacks

Coordinated cyber physical topology (CCPT) attacks are more dangerous to smart grids instead of purely physical or cyber topology attacks. CCPT attacks are categorized into physical topology and cyber-topology attacks [69]. In a physical topology attack, the attacker trips the transmission line, whereas in a cyber topology attack, the attacker misleads the control center, masks the outage signal of tripped line in the cyber layer, and generates a forged outage signal for another transmission line. Finally, the precise goal of the coordinated topology attack is to burden the critical line by deceiving the control center into making the wrong dispatch [112,113]. Furthermore, two types of unobservable cyberattacks on topology [114] are also investigated such as line-maintaining and line-removing. In the case of a line-maintaining attack, the adversary can modify measurements and line status data to make it appear that a line that is not in the system is now shown as lively at the control center through SCADA information; the reverse is accomplished by a line-removing attack. The adversary has the ability to modify the topology data or both state as well as topology data in line-removing and line-maintaining attacks. Another type of attack [112], state-preserving CCPT attacks, are examined, in which topology data are altered, whereas the states of the power system remain persistent. However, in [113] a more comprehensive consequence of CCPT attacks is established, where mutual topology and states can be altered. Researchers in [115] analyzed the vulnerabilities of the smart grid system to CCPT attacks. Despite that, future research directions demand defensive techniques and countermeasures against coordinated topology attacks.

4.9. Replay Attack

A replay attack (RA) is generated via stealing the information on a wireless communication network and mimicking it as a legitimate sender to deploy the stolen information to fabricate original information. This type of attack relies on historic data and creates trouble for the supervisor to notice the attack. Consequently, the attack leads to disturbing the power flow and time delays diverging frequencies. From an attacker's point of view, a replay attack can deliberately jam the system and is fully able to disrupt the diverse processes [116]. Stuxnet virus is used to launch the replay attack, which accessed the SCADA system that controls centrifuges. Accordingly, the centrifuge control system was modified and destroyed approximately 1000 centrifuges [117]. In the literature, a method for reflecting the replay attacks is proposed by adding some deliberate noise to control input, but it did not work well [118]. Another study [117] dynamically set the timing of accumulation of noise to the control input created on game theory. Accordingly, detection methods against RA such as nearest neighbor-based detection scheme, support vector model, and machine learning-based approach are elaborated in Table 9.

Table 9. Methods and countermeasures to defend against replay Attack.

Reference	Key Method	Explanation
[119]	Bargaining game	Replay attacks apparently threaten the smart grid system and need to be detected early. A Kalman filter is utilized to state the fault diagnosis matrix and then noise and control signal are included to present the properties of replay attack detection. Furthermore, based on the bargaining game method, noise is added to the control input with the knowledge of control performance and detection accuracy. At the end, through simulation, the efficiency of the proposed method is validated.
[120]	Support vector machine (SVM)	A data-driven approach is presented in which learning from classifier a labelled dataset is used, i.e., power state, to detect replay attack states from useful normal states. The support vector machine (SVM) is implemented as an ML classifier. To evaluate the effectiveness of the approach, IEEE bus systems are utilized and high detection accuracy is achieved.

Table 9. *Cont.*

Reference	Key Method	Explanation
[121]	Watermarking Technique	A novel improved watermarking technique is proposed to detect active replay attacks to smart grids. The suggested scheme makes use of the set-theoretic model predictive control framework to create a control input that can be securely and steadily connected to the utility grid for an a priori known number of steps, as and when they are needed. Results indicate that the watermarking technique efficiently detects the replay attack.
[122]	Proactive Intrusion Detection and Mitigation System (PIDMS)	PIDMS analyzes the both cyber and physical data streams in parallel in order to detect intrusion and implement the proactive response. Furthermore, PIDMS comprises ML algorithms and network IDS.

4.10. Malware Attacks

Cyberattacks on smart grid systems comprise malware attacks, including the Trojan horse malware Blackenergy, Stuxnet, and WannaCry Ransomware. In December 2015, an electricity outbreak occurred in Ukraine's Ivano-Frankivsk city, targeting the power grid as a cyberattack and affecting 80,000 people with a blackout. Consequently, it was found that this cyberattack was generated by using phishing email and BlackEnergy Trojan horse [123]. It has the ability to delete data, damage hard drives and control the systems. In the work of [44], authors address that defense against BlackEngery is not fully assured. However, applying certain precautions can reduce the risk of attack in the future. These precautions include methods such as following the antimalware, updating the firewall configurations, and upgrading the security patches as well. Furthermore, the implementation of Sandboxes can offer protection to test the applications and documents. However, these solutions are not suitable to apply to larger-scale companies. Similarly, another malware attack known as Stuxnet [124] exploits the SCADA system. Stuxnet can influence the programmable logic controllers (PLCs), which enabled it to penetrate inside the control system of an Iranian power plant. As a result, an upsurge in the rotation speed was caused, and the nuclear fuel was rapidly disrupted.

4.11. Other Cyberattacks

Other kinds of cyberattacks on smart grid systems include GPS spoofing attacks, zero dynamics attacks, and time synchronization attacks (TSA). In [125], authors elaborated on the TSA that disrupts the measurements collected from the grid. Furthermore, it leads to transmission line fault and voltage instability. Additionally, zero dynamics attacks consider the internal behavior of the grid system to control it maliciously and provide zero output. In order to generate a zero dynamics attack, a signal can be injected into the system to diverge the internal state, which is not noticeable from the mere observation [126]. Another cyberattack [127,128], a global positioning system (GPS) spoofing attack, in which PMU receives the GPS signals from diverse resources, is instigated in two ways. The first way is deceptive jamming, in which the attacker tries to mislead the receiver by transferring a fake GPS signal similar to the real one. The second way is known as repeater jamming, in which the attacker spoofs the GPS receivers by depending on the real signals captured frequently. In the work [128], the authors introduced the capsule neural network (CapsNet) to detect the GPS spoofing attack. CapsNet utilized the historical measurements from the smart grid system to train the model. Furthermore, temporal and spatial features are extracted and effectively separate the malicious and normal data.

5. Potential Solutions for Cybersecurity in Smart Grid

In this section, potential solutions against cyberattacks to smart grids are discussed comprehensively in terms of blockchain technology and artificial intelligence (AI) techniques including machine learning (ML) and deep learning (DL).

5.1. Blockchain Based Cybersecurity Techniques in Smart Grid

Blockchain technology has the capability to be applied in smart energy systems to self-regulate, mitigate cyberattacks, and manage the transactions and contracts. In traditional power systems, an attack is launched successfully if attackers tamper with the meter record, replace the data packages, make fraudulent energy trading payments, and hack the control center. However, blockchain provides solutions against smart grid cyberattacks: in Figure 5, the integration of blockchain in a smart grid is presented to pay the electricity purchase bill in a trustworthy and fair manner.

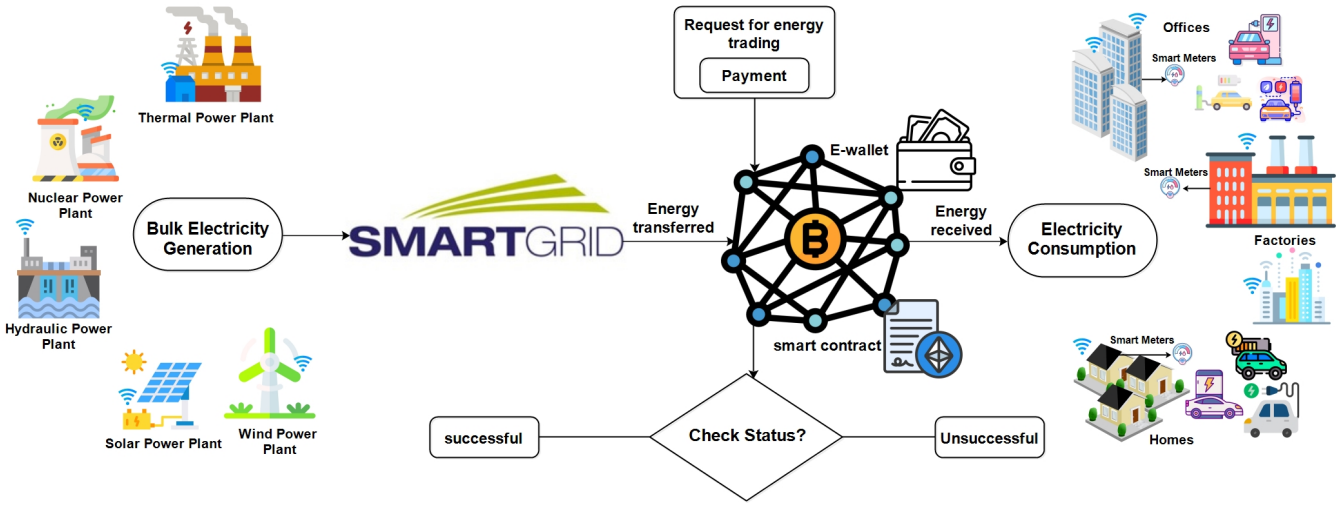

Figure 5. Adoption of blockchain in smart grid for secure energy trading.

In Table 10, a summary of works in the literature that aim to detect attacks based on blockchain for cybersecurity in smart grids including various features i.e., objective, type of attack, solution, consensus algorithms, deployment of Smart Contracts (SCs) and performance evaluation parameters is presented.

Kumari et al. [129], presented the ArMor to detect the malicious activities from AMI and SM based on the blockchain in smart grids. The integrity issues related to FDI attack and smart meter failures are successfully detected. In [130], a decentralized system is presented based on the Ethereum blockchain to mitigate the SPoF issue and DDoS attack. Authors [79], introduced the blockchain-based method for privacy preservation of energy exchange in smart grids. The PBFT consensus algorithm is deployed in blockchain based smart grid system. In [131], a decentralized scheme is presented based on the Bayesian inference to detect replay attacks and provides the regional data privacy. In [132], consensus-based method is proposed to increase the protection level of smart grid systems against cyberattacks.

Similarly, the authors of [133] exploit the blockchain to build trustworthy environment for smart grid components. The miners verify the transactions through investing their computational resources. GarliChain [134] is presented to solve the issue of anonymity and client's privacy during energy transfer in smart grids with the combination of garlic routing and blockchain. Furthermore, FeneChian [135], is introduced as blockchain-based energy trading scheme for better management, transparency, and verifiability in industrial IoT. All energy transfer transactions are done in an immutable nature with the protection of the client's rights. Reijsbergen et al. [136] designed a realistic threat model against a compromised smart grid to detect FDI attacks and provide an incentive for useful data upload that otherwise penalized operators if data were found to be malicious or incomplete.

Table 10. Blockchain based attack detection techniques for cybersecurity in smart grids.

Reference	Objective	Type of Attack	Solution	Consensus Algorithm	Blockchain Tool	Smart Contract Tool	Performance Evaluation
[129]	To propose a data analytics scheme, to identify malicious behavior in the SG system.	FDIA and SM failure	ARIMA and blockchain-based schemes to classify attacked/non-attacked, and reward to utility provider to deal with malicious activity.	-	Ethereum	Remix IDE	Prediction accuracy, latency, and data storage cost
[130]	Aim to control the smart meter attacks, protect them from unauthorized access and DDoS attacks.	DDoS	A decentralized architecture based on the blockchain in a distributed and trustworthy manner to deal with DDoS attacks.	-	Ethereum	Truffle framework	Flexibility, security and cost effectiveness
[79]	Aim to detect the network attacks and fraudulent transactions in smart grids.	Network attacks and fraudulent transactions	A blockchain-based scheme to achieve privacy with short signature, hash function for the exchange of energy between nodes and RNN for attack detection.	PBFT	-	-	Accuracy, detection rate and false alarm rate
[132]	Developed the blockchain-based decentralized mechanism against cyberattacks.	Coordinated replay attacks	Decentralized mechanism that relies on Bayesian inference with Ethereum-based blockchain.	PoA	Geth-based	Solidity	Computational performance and accuracy
[137]	To build the mechanism against PMU as it is susceptible to cyber-attacks due to their reliance on the GPS.	FDIAs	Consensus-based approach to improve the self-defensive capabilities of smart grids against cyberattacks.	-	-	-	Successful attack capability and probabilities
[133]	Detect the manipulation of meters' measurements that causes flawed decisions to be made in energy systems	FDIAs	Implementation of transparent public Blockchain-based SG data security	-	-	-	Accuracy, RMSE, MAE, and F1 score
[134]	Aim to solve the anonymity and privacy problem of consumers	SPoF and lack of trust	Implementation of garlic routing and consortium blockchain for privacy preservation during energy transfer in SGs.	PoA	-	-	Computational cost and path selection probability
[138]	To detect the identity-based security loop holes in the smart grid	Data manipulation and identity theft attacks	Blockchain-based identification and authentication technique to prevent identity theft and masquerading.	-	Hyperledger	-	Validation of the node in log(n)
[135]	Mitigate the cheating attack initiated by energy sellers, i.e., an energy seller refuses to transfer the energy to customer who already paid money.	Malicious energy purchasers	Blockchain-based energy trading scheme to assure the verifiable fairness of energy transfer.	PBFT	Ethereum, Ethereum-Wallet and Geth	-	Computational cost
[136]	Goal to design the secure SGs against FDI attacks	FDI attack	Blockchain based incentive method to reward operators for uploading authentic data and penalize if data is missing or malicious.	Round robin	Hyperledger Fabric	Go language	Anomaly detection rate

5.2. Artificial Intelligence Based Cybersecurity Techniques in Smart Grids

The artificial intelligence (AI) techniques in the smart grid for providing security are becoming more apparent. AI techniques have an ability to improve the reliability and robustness of smart grid systems. In this section, we presented the deep learning (DL)- and machine learning (ML)-based cybersecurity technique against smart grids attacks.

5.2.1. Deep Learning Based Cybersecurity Techniques in Smart Grids

Deep learning models comprise complex training tools developed to provide meaningful feature extractions when it is difficult in conventional methods due to the curse of dimensionality [139]. In context of cybersecurity in SGs, a wide range of deep learning methods have been implemented. In Figure 6, a general structure of the convolutional neural network (CNN) is depicted with two convolutional layers, two pooling layers, one hidden, fully convolution and output layer which is adopted in smart grids. However, in Table 11, multiple deep learning algorithms such as Recurrent Neural Networks (RNN), Artificial Neural Network (ANN), Deep Neural Network (DNN), etc., have been implemented in the literature to detect cyberattacks against smart grids.

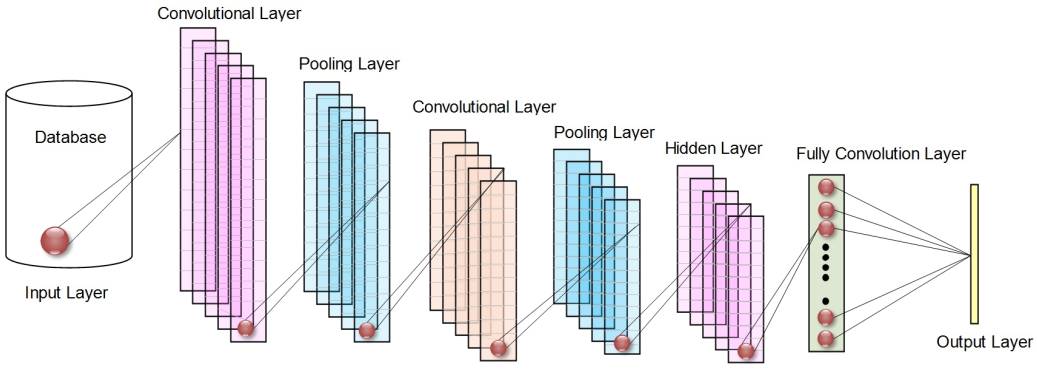

Figure 6. General structure of convolutional neural network (CNN) adopted in smart grids.

The authors of [69] presented the Kalman filter and recurrent neural network (KFRNN)-based technique to detect FDIA. The dynamic threshold is measured to detect the FDI attack. In [140], a detection technique is presented against FDIA that takes the input and output signals of a power-to-gas (PtG) and gas-fired generation (GfG) facility scheduler. Furthermore, hybrid neural network is implemented to detect FDIA without labeling the training data. Similarly, the authors of [141] detected the cyberattacks by implementing the deep learning techniques and targeted the IEC 61850 communication protocols. Yao et al. [142], introduced the energy theft detection framework as well as privacy preservation of energy in smart grid and CNN and Paillier algorithm. In the work of [143], authors presented the intrusion detection system (IDS) for IEEE 1815.1-based power system. A bidirectional RNN-based deep learning algorithm is employed to detect anomalies and verify the presented technique by testing various attacks, i.e., malware attack, FDI, and disabling reassembly (DR) attacks.

Siniosoglou et al. [144], introduced the IDS named as MENSA (anoMaly dEtection aNd claSsificAtion) based on the GAN architecture to detect anomalies and classify the Modbus and Distributed Network Protocol 3 (DNP3) attacks. He et al. [145], proposed the DL-based neural network model to detect FDI attack in terms of bypass the state estimation and causes for congestion of transmission lines in SG. In addition, researchers [146] exploited the ensemble-based DL method to identify the false readings. A couple of DL models are trained based on the samples derived from sliding window of the readings. Finally, best model is used in ensemble-based detector to identify the false readings. Moreover, researchers [147] introduced the DNN-based classification method for energy theft detection in smart grids. Through Bayesian optimizer, the hyperparameters are optimized, improving the performance of energy theft detection.

Table 11. Deep learning based attack detection techniques for cybersecurity in smart grids.

Reference	Type of Attack	Solution	DL Training Models	Dataset Generator	Implementation Tools	Performance Evaluation
[69]	FDIA	A two-level learner-based scheme with Kalman filter and recurrent neural network (KFRNN) is presented.	RNN	IEEE 14 Bus and IEEE 57 Bus	Matpower	MRSE, accuracy, F1 score, detection probability, false alarm rate
[140]	FDIA	A scheme based on the CNN and WT is proposed to detect attacks on the information received by the facility scheduler. Furthermore, hybrid neural network is presented to detect attacks on the output control signals.	WT, CNN and ANN	IEEE 30-bus	MATLAB	Identified as attacked, identified as normal, and detection accuracy
[141]	Inject, capture, replay, modify, drop, and delay attacks	Proposed and implemented the two-step deep learning model for cyberattack detection.	LSTM, RNN and GRU	IEEE 9-bus system	Testbed implementation	TPR, FNR, TNR, FPR, recall, precision, and F1-score
[142]	Energy theft	A combined CNN is used to detect abnormal behavior of the metering data. In addition, Paillier algorithm is deployed to protect the energy privacy.	CNN	Energy theft dataset from SGCC	Python, Numpy, Pandas, Keras and TensorFlow	Accuracy score
[143]	Malware, FDI and DR	An intrusion detection system with bidirectional RNN is presented for an IEEE 1815.1-based power system using CPS.	Bi-RNN	IEEE 1815.1	TensorFlow	-
[144]	Anomalies (i.e.,electricity measurements)	Presented the DL-based MENSA (anoMaly dEtection aNd claSsificAtion) for anomalies and cyberattacks.	GAN and DBN	Four datasets from the SPEAR project	Tshark, REST API, MTU, CICFlowMeter, and Suricata	Average accuracy, TPR, FPR and F1 score
[145]	FDI attacks	A simplified neural network is presented to detect FDI attacks targeting transmission line overflows.	NN	IEEE 118-bus system	MATPOWER 7.0	Accuracy, DR, precision, F1 score, FPR, ROC, and AUC
[146]	False readings in AMI	A general ensemble-based DL detector to enables the system operator to detect false readings in real time.	FFN, CNN, GRU, and LSTM	Smart Project Dataset	Python3, Numpy, Keras, Scikit-learn and Matplotlib	Accuracy, DR, FA, and HD
[147]	Electricity theft detection	DNN-based electricity theft detection method using time-domain features is presented.	DNN	SGCC dataset	-	TPR, Precision, F1 score, MCC, Accuracy and AUC ROC curve

5.2.2. Machine Learning-Based Cybersecurity Techniques in Smart Grids

Machine learning (ML)-based techniques are implemented in smart grids for providing mitigation and detection against cybersecurity attacks. The authors of [148] also implemented ML techniques to forecast electricity prices; however, we analyzed the ML techniques that are applied to detect the cyberattacks on smart meters that causes huge electricity cost. In Figure 7, we present the general framework adopted in smart grid. ML starts from the pre-processing of the dataset, and then features are extracted through Principal Component Analysis (PCA), kernel principal component analysis (KPCA), and Joint Mutual Information Maximization (JMIM) etc. After the extraction and selection of features, ML algorithms are applied and the model training is started; finally, based on the trained ML model, the results are achieved. In Table 12, a summary of ML algorithms applied in smart grids to detect cybersecurity attacks is elucidated.

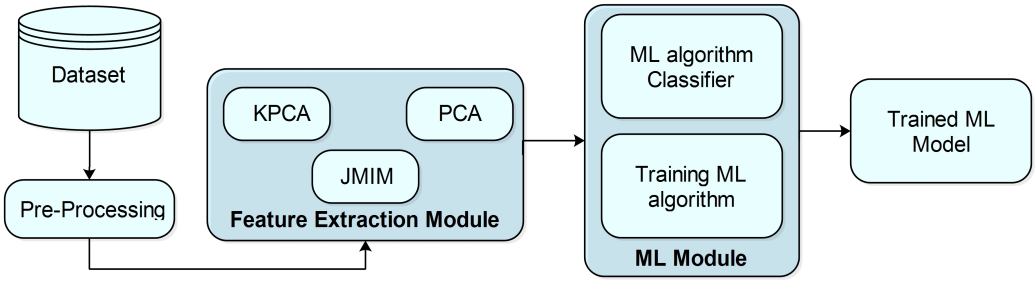

Figure 7. General Machine learning framework adopted in smart grid.

Ashrafuzzaman et al. [149] presented a machine learning-based technique to detect FDI attacks on state estimation. The ensemble learning is implemented with supervised and unsupervised classifiers to minimize the effect of the dimensionality reduction. In the work of [150], the authors analyzed the difference between physical grid and data manipulation change. The historical data are analyzed under concept drift with data distribution changes and computed through PCA. Lastly, K-NN algorithm is applied to show the effectiveness of presented scheme and achieved the highest accuracy. Furthermore, researchers [151] proposed the extremely randomized trees (ERT) algorithm with kernel principal component analysis (KPCA) to detect stealthy cyber-attacks. In the work of [63], authors employed the SVMLDT to detect the anomalies in smart grid. Moreover, adaptive load rejection scheme is implemented to mitigate the DoS attacks as well as remedial strategies are adopted accordingly under-attack situations.

Another anomaly detection and mitigation framework [152] is proposed, considering multiple data integrity attacks, i.e., pulse,ramp, replay-trip and replay attacks. Consequently, the ML algorithms such as KNN and DT are applied for attack classification and show accuracy of 96.5%. Similarly, in [153], a cyber–physical anomaly detection system (CPADS) is introduced in order to detect communication failure and data integrity attacks. The ML algorithm DT is applied with variational mode decomposition (VMD) to build a classification model. CPADS are evaluated on standard IEEE 39 bus system and measured performance. In addition, researchers [154,155] detected the FDI attacks based on the ensemble and extreme learning machines. In [154], optimized feature sets are extracted to label the behavior of FDIA and a focal-loss-lightGBM (FLGB) ensemble classifier is developed to detect FDIA automatically. To improve the performance of extreme learning machines (ELMs), Gaussian random distribution is deployed to initialize the weights [155]. A hierarchical clustering method is proposed in order to detect the FDI and DoS attacks, which interrupts the state estimation process. The DT algorithm is implemented to remove the threat and Kalman filters are used to provide speedy and accurate process [156]. Likewise, the authors of [157] detected the FDI attacks based on the ML methods such as visualization, classification, and clustering.

Table 12. Machine learning based attack detection techniques for cybersecurity in smart grids.

Reference	Type of Attack	Solution	Feature Selection	ML Training Models	Dataset Generator	Implementation Tools	Performance Evaluation
[149]	FDIA	A data-driven ML-based scheme to detect stealthy FDIA on state estimation.	RFC	LR, DT, NB, NN, SVM, LOF, ISOF and EE	IEEE 14-bus system	MATPOWER	F1-Score, Accuracy, Precision, Sensitivity, FPR, Specificity, ROC AUC
[150]	FDIA	Analyze the historical data by concept drift and focus on the distribution change. The dimensionality reduction and statistical hypothesis testing are implemented.	PCA	KNN	IEEE 14-bus system	MATPOWER, MATLAB 2017 and Python 3	F-measure and FPR
[151]	Stealthy cyber-attack (SCA)	KPCA technique is applied to transform the data into a lower-dimensional space. The data transformed by KPCA become the input for the ERT to detect SCA attacks.	KPCA	ERT	IEEE 57 and 118-bus systems	Matpower	Accuracy, ROC curves, and ROC AUC
[63]	DoS	A multi-class classification algorithm employed for anomaly detection in smart grid.	-	SVM and DT	IEEE 39-bus system	Testbed-based implementation	-
[152]	Pulse, ramp, relay-trip, and replay attack	Anomaly detection (AD) with supervised ML and model-based mitigation. With physics and signal entropy-based feature extraction increased the robustness and detection accuracy of ML model.	PCA	KNN and DT	2-area of 4-machine	Testbed-based implementation	Accuracy
[153]	FDIA	A CPADS (cyber–physical anomaly detection system) developed with PMU measurements, network packet properties and ML algorithms.	Rules-based	VMD and DT	IEEE 39-bus system	Testbed-based implementation	Accuracy, AR, AP, and AF
[154]	FDIA	A novel FDIA detection model based on ensemble learning with optimal feature extraction and a FLGB ensemble classifier is employed.	JMIM	Ensemble classifier	Public Google power system cyber-attack dataset	-	Accuracy, FPR, ROC curve, and AUC
[155]	FDIA	A classifier is developed by aggregating a series of extreme learning machines (ELMs) to detect anomalies caused by FDIAs.	-	GRD, LHS and ensemble ELM	IEEE 14-bus and IEEE 57-bus	MATLAB R2014a	Classification accuracy

6. Emerging Technologies and Future Research Directions

From the above discussion in different parts of the papers, smart grids are vulnerable to cyberattacks. Similarly, some papers have discussed the safety and associated vulnerabilities in smart grids. As a result, the security and privacy can be enforced by inducing wide range of tools and technologies. To improve the security measures of smart grids, it is recommended to analyze the cyberattacks with their dynamic nature, attack mechanism, and the key factors of cyberattacks on smart grids. This analysis enforces the discovery of new types of attacks and vulnerabilities which can ultimately strengthen the smart grids following a more resilient and robust system. In this section, we will discuss various future research directions and opportunities to obtain the advanced secure smart grid systems.

- Communication infrastructure in smart grid security: The network and communication model should be strengthened through advanced security measures which should be imposed during data collection and interchange phase. Furthermore, the vendors should follow the standards to make use of distribution devices in the communication phase to avoid interoperability issues. Consequently, the providers/vendors can build their protocols as open-source so that other vendors should anticipate in existing code and follow the same standard while manufacturing their own security tools. Being open-source, bug fixes and security vulnerability checks can also be easily verified and corrected as the community is taking part in the development and testing process. As a result of this collaboration, the security product will support the implementation of security tools by default in the communication network of the smart grid, which will ultimately enforce the standard security policies available on all devices that are participating in the grid communication network.
- High-level security algorithms to detect attacks: For implementing more enhanced security mechanisms, extra effort is required to target higher-level algorithms or data structures. As a result, the current state estimator algorithms cannot identify improper/defective data using the existing detection techniques available in the FDIAs, therefore high-level security data structures and algorithms are needed. For instance, apart from the existing bad data detection steps, if the SCADA system consists of other security modules, which are solely used to diagnose the false positive rates with the help of new regulation, it would better harden the security breaches by the attackers. Consequently, the additional work is required to enrich the impact analysis of FDIA on the distribution and use side, respectively. Apart from transmission systems, the distribution end can also be affected by showing false meter readings and fake topology information. Similarly, the meters installed at user premises that are used to transmit user consumption measures can also be hacked and manipulated. As a result, the load management and demand side management security measures should keenly be focused in the future.
- Federated learning in smart grids: Currently, federated learning (FL) is appealing as a privacy-preserving paradigm as it trained the AI models in a collaborative manner by inviting underlying devices. The privacy of each device is protected by localizing the training of model in comparison with ML where raw data are sent to the main server [158]. FL applications for the smart grid include electric load forecasting, energy demand prediction, and data privacy of a large power system. In addition, federated learning has been successfully implemented in various fields, i.e., health care, smart cities, transportation, finance, visual object detection, next-word prediction, and so on. Similarly, in [159] authors applied FL to share the private energy data of users in smart grid to achieve privacy and efficient communication. However, FL surface is also facing challenges and is prone to cybersecurity attacks mentioned by various researchers [160,161]. Before the implementation of FL into smart grid, it is necessary to consider robust security measures in the future.
- Blockchain technology for securing smart grids: As blockchain technology is still immature, case-by-case analysis of regulatory frameworks in terms of security is necessary. The electricity flowing through the wires to the home is similar as it

passes by a burning coal or a solar array. Therefore, authenticating and tracing the energy source is a huge challenge. The embedded security features in blockchain technology can be emerged with the smart grids to enforce efficient and secure power transmission and management. As blockchain technology implements security using public/private key encryption methods with key access, everyone who tries to breach the system would encounter authentication through a secure credentials system in order to access system's operational resources over the network. Consequently, the blockchain technology is an essential approach to make power grid safe if the access key codes are kept secure and safe. Overall, in order to prevent malicious attacks and make hacking more difficult for intruders, secure and efficient smart cities must be used as backbone. Furthermore, blockchain features such as the immutability and decentralization of data lead to permanent storage; hence, one must be careful when implementing smart contracts, as any malfunction or misconduct can be observed within the system [162].

- Big data integration in smart grids: The big data (BD) collected from smart grids is key information that could be extensively beneficial for different smart grid applications, such as load profiling and demand response. However, a security vulnerability in decision-making techniques may cause the unauthorized gain of full access to a customer's data. On the other hand, a secure approach for decision making can provide enormous satisfaction to all the stakeholders, i.e., utility providers and consumers. The prospective research in big data is diverse when used in smart grids. Big data supports various solutions to the directional flow of data/information and analyzing and processing that information. Similarly, with the big data solutions, demand-side management has become a crucial activity for managing the stockholders in power systems. As a result, the learned behaviors of consumer actions and power consumption can enormously help to demand response activities on the customers' end, which is also known as consumer behavior predictions.
- Smart grid security with AI and 5G: Major changes have been posted on smart grids through the latest technologies introduced by AI and 5G. Indeed, 5G and B5G (Beyond5G) technology would be a powerful tool to govern high-speed and reliable communication to perform real-time grid monitoring via Internet of things (IoT). However, with the advent of this technology, new challenges are ahead [163]. AI and Machine learning algorithms are promising options to intelligently operate the network with reliability, network efficiency, robustness goals, and can obtain the Quality of Service (QoS) demands as expected. Enriched historical data are required to train model in order to ensure the model's accuracy and mitigate the over/under fitting issues of AI model in smart grid. Furthermore, it should provide the guarantee of controlling the decisions of AI models to align with the cybersecurity constraints of power systems.
- Cyber resilience of smart grid SoS: The entire smart grid network is considered as a system of systems (SoS) that integrates the legacies, new systems, and produces new goals beyond the distinct systematic competencies. Any breakdown occurred in the smart grid subsystem will have an impact on the entire smart grid system of systems. The implementation of a secure smart grid system of systems is now essential and a high research priority. To address this challenge, in the future extended Bayesian model can be developed, and utilize the analysis techniques, i.e., information theory, to improve the overall smart grid resilience system. Furthermore, the time-dependent dynamic Bayesian model can be integrated to observe the system performance and uniformity of the model with the passage of time [164].

7. Conclusions

Cyber threats targeting smart grid security are a critical issue and face several challenges from a multitude of attacks. In this paper, the smart grid threats covered the two core domains: the intrinsic vulnerability of the system and the external cyberattacks. Smart grid

vulnerabilities are elaborated in all aspects, including their components; data management, services, and applications; running environment; and evolving and complex smart grid vulnerabilities. Furthermore, we included a global review of cyberattack incidents witnessed against smart grids between 2010 and July 2022 with diverse characteristics such as attack location, range, type of attack, and consequences. The in-depth thematic taxonomy of cyberattacks on smart grids is investigated with state-of-the-art approaches presented with their attack strategy, consequences, and detection methods. Furthermore, potential solutions for cyberattacks on smart grids are discussed expansively in terms of blockchain technology and artificial intelligence (AI) techniques. Though the aforementioned solutions effectively detect cyberattacks over smart grids, however, a couple of challenges—particularly fake topology information, identification of defective data, security vulnerabilities, integration of big data, blockchain, and so on—still endure. Therefore, from the perspective of emerging technologies, future research directions are provided for the robust cybersecurity of smart grids against erudite cyberattacks, as new attack tactics are endlessly exposed.

Author Contributions: Conceptualization, J.D. and A.Q.; funding acquisition, J.D.; methodology, J.D., A.Q. and Z.Z.; investigation, J.D. and H.N.; supervision, J.D. and H.N.; writing—original draft preparation, J.D., A.Q., Z.Z. and A.K.; writing—review and editing, A.Q. All authors have read and agreed to the published version of the manuscript.

Funding: These materials are a result of research supported by The European Union—The Internal Security Fund (ISF), A431.678/2016.

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

Abbreviations

The following abbreviations are used in this manuscript:

AAA	Authentication, Authorization, and Accounting
ANN	Artificial Neural Network
AUC	Area Under Curve
AMI	Advanced Metering Infrastructure
API	Application Programming Interface
ABOD	Angle-based Outlier Detector
ARP	Address Resolution Protocol
CPS	Cyber–Physical System
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CNN	Convolutional Neural Network
CIA	Confidentiality, Integrity, and Availability
COSEM	Companion Specification for Energy Metering
CRM	Customer Relationship Management
DNN	Deep Neural Network
DMZ	DeMilitarized Zone
DBN	Deep Belief Networks
DER	Distributed Energy Resources
DR	Detection rate
FA	False Alarm
DNP3	Distributed Network Protocol 3
DLMS	Device Language Message Specification
DWT	Discrete wavelet transform
DT	Decision Tree
DBSCAN	Density-Based Spatial Clustering of Applications with Noise
ERT	Extremely Randomized Trees
EE	Elliptic Envelope
ERP	Enterprise Resource Planning

FTP	File Transfer Protocol
FFN	Feed-Forward Neural Network
FNR	False Negative Rate
FPR	False Positive Rate
FLGB	Focal-Loss-lightgbm
GRU	Gated Recurrent Unit Network
GAN	Generative Adversarial Networks
GRD	Gaussian Random Distribution
HD	Highest difference
HBOS	Histogram-base Outlier Detection
HTTPS	Hyper Text Transfer Protocol over SecureSocket Layer
HMI	Human Machine Interface
IDE	Integrated Dynamic Environment
IF	Isolation Forest
ICCP	Inter Control Center Protocol
ICMP	Internet Control Message Protocol
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
KNN	K-Nearest Neighbor
KPCA	Kernel Principal Component Analysis
JMIM	Joint Mutual Information Maximization
LSTM	Long Short-Term Memory Network
LR	Logistic Regression
LOF	Local Outlier Factor
LHS	Latin Hypercube Sampling
LSCP	Locally Selective Combination
MAE	Mean Absolute Error
MRSE	Mean Relative Square Error
MTU	Master Terminal Unit
MCC	Matthews Correlation Coefficient
NB	Naive Bayes
NN	Neural Network
NTP	Network Time Protocol
NVD	National Vulnerability Database
OT	Operational Technology
PoA	Proof-of-Authority
PBFT	Practical Byzantine Fault Tolerance
PCA	Principal Component Analysis
RNN	Recurrent Neural Networks
RMSE	Root Mean Square Error
RNN	Recurrent Neural Networks
REST	Representational State Transfer
ROC	Receiver Operator Characteristic
RFC	Random forest classifier
RTU	Remote Terminal Unit
SGCC	State Grid Corporation of China
SPEAR	Secure and PrivatE smArt gRid
SCADA	Supervisory Control And Data Acquisition
SIEM	Security Information and Event Management
SVM	Support Vector Machine
TP	True Positive
TNR	True Negative Rate
TASE.2	Telecontrol Application Service Element 2
VMD	Variational Mode Decomposition
VULDB	Vulnerability Database

References

1. GlobalNewswire. The $39.9 Billion Worldwide Substation Automation Industry Is Expected to Reach $54.2 Billion by 2026. Available online: https://www.globenewswire.com/news-release/2021/06/04/2241918/28124/en/The-39-9-Billion-Worldwide-Substation-Automation-Industry-is-Expected-to-Reach-54-2-Billion-by-2026.html (accessed on 22 January 2022).
2. Nations, U. What Is Renewable Energy? Available online: https://www.un.org/en/climatechange/what-is-renewable-energy (accessed on 1 August 2022).
3. Solaun, K.; Cerdá, E. Climate change impacts on renewable energy generation. A review of quantitative projections. *Renew. Sustain. Energy Rev.* **2019**, *116*, 109415. [CrossRef]
4. Abrahamsen, F.E.; Ai, Y.; Cheffena, M. Communication Technologies for Smart Grid: A Comprehensive Survey. *Sensors* **2021**, *21*, 8087. [CrossRef] [PubMed]
5. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2020**, *169*, 107094. [CrossRef]
6. 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]
7. NISTIR. Guidelines for Smart Grid Cybersecurity. Available online: https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf (accessed on 22 January 2022).
8. Tufail, S.; Parvez, I.; Batool, S.; Sarwat, A. A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid. *Energies* **2021**, *14*, 5894. [CrossRef]
9. Rawat, D.B.; Bajracharya, C. Cyber security for smart grid systems: Status, challenges and perspectives. In Proceedings of the SoutheastCon 2015, Fort Lauderdale, FL, USA, 9–12 April 2015. [CrossRef]
10. 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]
11. SmartGrid.gov. The Smart Grid. Available online: https://www.smartgrid.gov/the_smart_grid/smart_grid.html (accessed on 22 January 2022).
12. NIST. National Vulnerability Database. Available online: https://nvd.nist.gov/ (accessed on 5 August 2022).
13. U.S.D. of Energy. "GRID 2030" A National Vision Forelectricity's Second 100 Years. Available online: https://www.energy.gov/sites/default/files/oeprod/DocumentsandMedia/Electric_Vision_Document.pdf (accessed on 22 January 2022).
14. Office of Electricity. The Smart Grid: An Introduction. Available online: https://www.energy.gov/oe/downloads/smart-grid-introduction-0 (accessed on 22 January 2022).
15. Hahn, A. Operational Technology and Information Technology in Industrial Control Systems. In *Advances in Information Security*; Springer International Publishing: Cham, Switzerland, 2016; pp. 51–68. [CrossRef]
16. Zhang, Z.; Yin, R.; Ning, H. Internet of Brain, Thought, Thinking, and Creation. *Chin. J. Electron.* **2022**, *31*, 1–18.
17. Gaushell, D.J.; Darlington, H.T. Supervisory control and data acquisition. *Proc. IEEE* **1987**, *75*, 1645–1658. [CrossRef]
18. Zhang, Z.; Ning, H.; Shi, F.; Farha, F.; Xu, Y.; Xu, J.; Zhang, F.; Choo, K.K.R. Artificial intelligence in cyber security: Research advances, challenges, and opportunities. *Artif. Intell. Rev.* **2021**, *55*, 1029–1053. [CrossRef]
19. Upadhyay, D.; Sampalli, S. SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. *Comput. Secur.* **2020**, *89*, 101666. [CrossRef]
20. Ning, H.; Zhang, Z.; Daneshmand, M. PhiNet of Things: Things Connected by Physical Space From the Natural View. *IEEE Internet Things J.* **2021**, *8*, 8680–8692. [CrossRef]
21. Ning, H.; Ye, X.; Bouras, M.A.; Wei, D.; Daneshmand, M. General Cyberspace: Cyberspace and Cyber-Enabled Spaces. *IEEE Internet Things J.* **2018**, *5*, 1843–1856. [CrossRef]
22. Huang, Y.; Lu, Y.; Wang, F.; Fan, X.; Liu, J.; Leung, V.C. An Edge Computing Framework for Real-Time Monitoring in Smart Grid. In Proceedings of the 2018 IEEE International Conference on Industrial Internet (ICII), Seattle, WA, USA, 21–23 October 2018. [CrossRef]
23. Bui, N.; Castellani, A.; Casari, P.; Zorzi, M. The internet of energy: A web-enabled smart grid system. *IEEE Netw.* **2012**, *26*, 39–45. [CrossRef]
24. Kafle, Y.R.; Mahmud, K.; Morsalin, S.; Town, G.E. Towards an internet of energy. In Proceedings of the 2016 IEEE International Conference on Power System Technology (POWERCON), Wollongong, NSW, Australia, 28 September–1 October 2016. [CrossRef]
25. Piggin, R. Industrial systems: Cyber-security's new battlefront. *Eng. Technol.* **2014**, *9*, 70–74. doi: 10.1049/et.2014.0810. [CrossRef]
26. Anand, P.; Singh, Y.; Selwal, A.; Singh, P.K.; Felseghi, R.A.; Raboaca, M.S. IoVT: Internet of Vulnerable Things? Threat Architecture, Attack Surfaces, and Vulnerabilities in Internet of Things and Its Applications towards Smart Grids. *Energies* **2020**, *13*, 4813. [CrossRef]
27. Xie, J.; Stefanov, A.; Liu, C.C. Physical and Cybersecurity in a Smart Grid Environment. In *Advances in Energy Systems: The Large-Scale Renewable Energy Integration Challenge*; Wiley: Hoboken, NJ, USA, 2019; pp. 85–109. [CrossRef]
28. Mathas, C.M.; Vassilakis, C.; Kolokotronis, N.; Zarakovitis, C.C.; Kourtis, M.A. On the Design of IoT Security: Analysis of Software Vulnerabilities for Smart Grids. *Energies* **2021**, *14*, 2818. [CrossRef]
29. Vuldb. Vulnerability Database. Available online: https://vuldb.com/ (accessed on 5 August 2022).
30. Details, C. Common Vulnerabilities and Exposures. Available online: https://www.cvedetails.com/ (accessed on 5 August 2022).
31. O'Driscoll, A. Cyber Security Vulnerability Statistics and Facts of 2022. Available online: https://www.comparitech.com/blog/information-security/cybersecurity-vulnerability-statistics/ (accessed on 22 January 2022).

32. First Common Vulnerability Scoring System SIG. Available online: https://www.first.org/cvss/ (accessed on 5 August 2022).
33. Lázaro, J.; Astarloa, A.; Rodríguez, M.; Bidarte, U.; Jiménez, J. A Survey on Vulnerabilities and Countermeasures in the Communications of the Smart Grid. *Electronics* **2021**, *10*, 1881. [CrossRef]
34. Xu, Y.; Yang, Y.; Li, T.; Ju, J.; Wang, Q. Review on cyber vulnerabilities of communication protocols in industrial control systems. In Proceedings of the 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, China, 26–28 November 2017. [CrossRef]
35. ENISA. Smart Grid Security—Annex II. Security Aspects of the Smart Grid. Available online: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering/ENISA_AnnexII-SecurityAspectsofSmartGrid.pdf (accessed on 5 August 2022).
36. ENISA. ENISA Smart Grid Security Recommendations. Available online: https://www.enisa.europa.eu/publications/ENISA-smart-grid-security-recommendations (accessed on 5 August 2022).
37. Krause, T.; Ernst, R.; Klaer, B.; Hacker, I.; Henze, M. Cybersecurity in Power Grids: Challenges and Opportunities. *Sensors* **2021**, *21*, 6225. [CrossRef]
38. Alonso, M.; Turanzas, J.; Amaris, H.; Ledo, A.T. Cyber-Physical Vulnerability Assessment in Smart Grids Based on Multilayer Complex Networks. *Sensors* **2021**, *21*, 5826. [CrossRef]
39. Borenius, S.; Gopalakrishnan, P.; Tjernberg, L.B.; Kantola, R. Expert-Guided Security Risk Assessment of Evolving Power Grids. *Energies* **2022**, *15*, 3237. [CrossRef]
40. Cartwright, J. Europe's Power Grids Readied against Cyber Attack. Available online: https://ec.europa.eu/research-and-innovation/en/horizon-magazine/europes-power-grids-readied-against-cyber-attack (accessed on 22 January 2022).
41. Wikipedia. Stuxnet. Available online: https://en.wikipedia.org/wiki/Stuxnet#:~:text=Stuxnet%20reportedly%20ruined%20almost%20one,1%2C000%20machines%20to%20physically%20degrade (accessed on 22 January 2022).
42. NERC. September 2011 Southwest Blackout Event. Available online: https://www.nerc.com/pa/rrm/ea/Pages/September-2011-Southwest-Blackout-Event.aspx#:~:text=OntheafternoonofSeptember,,andBajaCalifornia,Mexico (accessed on 22 January 2022).
43. Ju-min Park, M.C. South Korea Blames North Korea for December Hack on Nuclear Operator. Available online: https://www.reuters.com/article/us-nuclear-southkorea-northkorea-idUSKBN0MD0GR20150317 (accessed on 22 January 2022).
44. Khan, R.; Maynard, P.; McLaughlin, K.; Laverty, D.; Sezer, S. Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid. In Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research 2016, Belfast, UK, 23–25 August 2016; pp. 53–63.
45. Wei, L.; Gao, D.; Luo, C. False Data Injection Attacks Detection with Deep Belief Networks in Smart Grid. In Proceedings of the 2018 Chinese Automation Congress (CAC), Xi'an, China, 30 November–2 December 2018. [CrossRef]
46. Androjna, A.; Twrdy, E. Cyber threats to maritime critical infrastructure. In *Cyber Terrorism and Extremism as Threat to Critical Infrastructure Protection*; Ministry of Defence Republic of Slovenia: Ljubljana, Slovenia, 2020.
47. Detwiler, B. Ukraine Cybersecurity Conference Highlighted New Threats a Week before the Petya Ransomware Attack. Available online: https://www.techrepublic.com/article/ukraine-cybersecurity-conference-highlighted-new-threats-a-week-before-the-petya-ransomware-attack/ (accessed on 22 January 2022).
48. News, C.H. Hackers Hit French Firm Ingerop Stealing 65 GB Data Relating to Nuclear Power Plants. Available online: https://cyware.com/news/hackers-hit-french-firm-ingerop-stealing-65-gb-data-relating-to-nuclear-power-plants-f193b9ba/ (accessed on 22 January 2022).
49. Harper, C. First Ever DoS Cyber-Attack on a US Power Grid Detailed In Startling Report. Available online: https://hothardware.com/news/dos-us-power-grid (accessed on 22 January 2022).
50. News, B. Ransomware Hits Johannesburg Electricity Supply. Available online: https://www.bbc.com/news/technology-49125853 (accessed on 22 January 2022).
51. Winder, D. Bitcoin Hackers Charged as Nuclear Power Plant Security Compromised. Available online: https://www.forbes.com/sites/daveywinder/2019/08/23/bitcoin-hackers-charged-as-nuclear-power-plant-security-compromised/?sh=407f199e2735 (accessed on 22 January 2022).
52. He, S.; Zhou, Y.; Lv, X.; Chen, W. Detection Method for Tolerable False Data Injection Attack Based on Deep Learning Framework. In Proceedings of the 2020 Chinese Automation Congress (CAC), Shanghai, China, 6–8 November 2020; pp. 6717–6721.
53. Toulas, B. Energias de Portugal (EDP) Fell Victim to the "Ragnar Locker" Ransomware. Available online: https://www.technadu.com/energias-de-portugal-edp-fell-victim-to-ragnar-locker-ransomware/98913/ (accessed on 22 January 2022).
54. BleepingComputer. Power Company Enel Group Suffers Snake Ransomware Attack. Available online: https://www.bleepingcomputer.com/news/security/power-company-enel-group-suffers-snake-ransomware-attack/ (accessed on 22 January 2022).
55. BleepingComputer. Netwalker Ransomware Hits Pakistan's Largest Private Power Utility. Available online: https://www.bleepingcomputer.com/news/security/netwalker-ransomware-hits-pakistans-largest-private-power-utility/ (accessed on 22 January 2022).
56. Esposito, D.; Gimon, E. The Texas Big Freeze: How Much Were Markets to Blame for Widespread Outages? Available online: https://www.utilitydive.com/news/the-texas-big-freeze-how-much-were-markets-to-blame-for-widespread-outages/601158/ (accessed on 22 January 2022).

57. IronNet. Industroyer2 Malware Targeting Ukrainian Energy Company. Available online: https://www.ironnet.com/blog/industroyer2-malware-targeting-ukrainian-energy-company (accessed on 22 January 2022).
58. Liu, Y.; Ning, P.; Reiter, M.K. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur.* **2011**, *14*, 1–33. [CrossRef]
59. Wang, Q.; Tai, W.; Tang, Y.; Ni, M. A review on false data injection attack toward cyber-physical power system. *Acta Autom. Sin.* **2019**, *45*, 7283.
60. Che, L.; Liu, X.; Li, Z.; Wen, Y. False Data Injection Attacks Induced Sequential Outages in Power Systems. *IEEE Trans. Power Syst.* **2019**, *34*, 1513–1523. [CrossRef]
61. Liu, X.; Li, Z.; Liu, X.; Li, Z. Masking Transmission Line Outages via False Data Injection Attacks. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 1592–1602. [CrossRef]
62. Tan, R.; Nguyen, H.H.; Foo, E.Y.S.; Dong, X.; Yau, D.K.Y.; Kalbarczyk, Z.; Iyer, R.K.; Gooi, H.B. Optimal False Data Injection Attack against Automatic Generation Control in Power Grids. In Proceedings of the 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS), Vienna, Austria, 11–14 April 2016. [CrossRef]
63. Wang, S.; Bi, S.; Zhang, Y.J.A. Locational Detection of the False Data Injection Attack in a Smart Grid: A Multilabel Classification Approach. *IEEE Internet Things J.* **2020**, *7*, 8218–8227. [CrossRef]
64. Prasanna Srinivasan, V.; Balasubadra, K.; Saravanan, K.; Arjun, V.S.; Malarkodi, S. Multi Label Deep Learning classification approach for False Data Injection Attacks in Smart Grid. *KSII Trans. Internet Inf. Syst.* **2021**, *15*, 2168–2187.
65. Singh, S.K.; Khanna, K.; Bose, R.; Panigrahi, B.K.; Joshi, A. Joint-Transformation-Based Detection of False Data Injection Attacks in Smart Grid. *IEEE Trans. Ind. Inform.* **2018**, *14*, 89–97. [CrossRef]
66. Huang, K.; Xiang, Z.; Deng, W.; Yang, C.; Wang, Z. False Data Injection Attacks Detection in Smart Grid: A Structural Sparse Matrix Separation Method. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 2545–2558. [CrossRef]
67. Tang, B.; Yan, J.; Kay, S.; He, H. Detection of false data injection attacks in smart grid under colored Gaussian noise. In Proceedings of the 2016 IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA, USA, 17–19 October 2016. [CrossRef]
68. Zhang, G.; Li, J.; Bamisile, O.; Cai, D.; Hu, W.; Huang, Q. Spatio-Temporal Correlation-Based False Data Injection Attack Detection Using Deep Convolutional Neural Network. *IEEE Trans. Smart Grid* **2022**, *13*, 750–761. [CrossRef]
69. Wang, Y.; Zhang, Z.; Ma, J.; Jin, Q. KFRNN: An Effective False Data Injection Attack Detection in Smart Grid Based on Kalman Filter and Recurrent Neural Network. *IEEE Internet Things J.* **2021**, *9*, 6893–6904. [CrossRef]
70. Dehghani, M.; Ghiasi, M.; Niknam, T.; Kavousi-Fard, A.; Shasadeghi, M.; Ghadimi, N.; Taghizadeh-Hesary, F. Blockchain-Based Securing of Data Exchange in a Power Transmission System Considering Congestion Management and Social Welfare. *Sustainability* **2020**, *13*, 90. [CrossRef]
71. Yi, P.; Zhu, T.; Zhang, Q.; Wu, Y.; Li, J. A denial of service attack in advanced metering infrastructure network. In Proceedings of the 2014 IEEE International Conference on Communications (ICC), Sydney, Australia, 10–14 June 2014. [CrossRef]
72. Guo, Y.; Ten, C.W.; Hu, S.; Weaver, W.W. Modeling distributed denial of service attack in advanced metering infrastructure. In Proceedings of the 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 18–20 February 2015. [CrossRef]
73. Taft, J. Assessment of Existing Synchrophasor Networks. Available online: https://www.naspi.org/sites/default/files/reference_documents/pnnl_27557_assess_existing_synchrophasor_net.pdf (accessed on 22 January 2022).
74. 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]
75. Wang, K.; Du, M.; Maharjan, S.; Sun, Y. Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart Grid. *IEEE Trans. Smart Grid* **2017**, *8*, 2474–2482. [CrossRef]
76. Zhe, W.; Wei, C.; Chunlin, L. DoS attack detection model of smart grid based on machine learning method. In Proceedings of the 2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS), Shenyang, China, 28–30 July 2020. [CrossRef]
77. Hasnat, M.A.; Rahnamay-Naeini, M. A Data-Driven Dynamic State Estimation for Smart Grids under DoS Attack using State Correlations. In Proceedings of the 2019 North American Power Symposium (NAPS), Wichita, KS, USA, 13–15 October 2019. [CrossRef]
78. Mahmood, H.; Mahmood, D.; Shaheen, Q.; Akhtar, R.; Changda, W. S-DPS: An SDN-Based DDoS Protection System for Smart Grids. *Secur. Commun. Netw.* **2021**, *2021*, 6629098. [CrossRef]
79. Ferrag, M.A.; Maglaras, L. DeepCoin: A Novel Deep Learning and Blockchain-Based Energy Exchange Framework for Smart Grids. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1285–1297. [CrossRef]
80. Radoglou-Grammatikis, P.I.; Sarigiannidis, P.G. Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems. *IEEE Access* **2019**, *7*, 46595–46620. [CrossRef]
81. Kim, J.; Tong, L.; Thomas, R.J. Data Framing Attack on State Estimation. *IEEE J. Sel. Areas Commun.* **2014**, *32*, 1460–1470. [CrossRef]
82. Wang, J.; Hui, L.C.K.; Yiu, S.M. Data Framing Attacks against Nonlinear State Estimation in Smart Grid. In Proceedings of the 2015 IEEE Globecom Workshops (GC Wkshps), San Diego, CA, USA, 6–10 December 2015. [CrossRef]

83. Jiao, W.; Li, V.O.K. Support Vector Machine Detection of Data Framing Attack in Smart Grid. In Proceedings of the 2018 IEEE Conference on Communications and Network Security (CNS), Beijing, China, 30 May–1 June 2018. [CrossRef]
84. Drias, Z.; Serhrouchni, A.; Vogel, O. Taxonomy of attacks on industrial control protocols. In Proceedings of the 2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS), Paris, France, 22–24 July 2015. [CrossRef]
85. Kayastha, N.; Niyato, D.; Hossain, E.; Han, Z. Smart grid sensor data collection, communication, and networking: A tutorial. *Wirel. Commun. Mob. Comput.* **2012**, *14*, 1055–1087. [CrossRef]
86. Crane, C. 80 Eye-Opening Cyber Security Statistics for 2019. Available online: https://www.thesslstore.com/blog/80-eye-opening-cyber-security-statistics-for-2019/ (accessed on 22 January 2022).
87. Deb, D.; Chakraborty, S.R.; Lagineni, M.; Singh, K. Security Analysis of MITM Attack on SCADA Network. In *Communications in Computer and Information Science*; Springer: Singapore, 2020; pp. 501–512. [CrossRef]
88. Swales, A. Open modbus/tcp specification. *Schneider Electr.* **1999**, *29*, 3–19.
89. Konstantinou, C.; Sazos, M.; Maniatakos, M. FLEP-SGS2: A Flexible and Low-cost Evaluation Platform for Smart Grid Systems Security. In Proceedings of the 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 18–21 February 2019. [CrossRef]
90. Kulkarni, S.; Rahul, R.K.; Shreyas, R.; Nagasundari, S.; Honnavalli, P.B. MITM Intrusion Analysis for Advanced Metering Infrastructure Communication in a Smart Grid Environment. In *Communications in Computer and Information Science*; Springer International Publishing: Cham, Switzerland, 2020; pp. 256–267. [CrossRef]
91. Varmaziari, H.; Dehghani, M. Cyber Attack Detection in PMU Networks Exploiting the Combination of Machine Learning and State Estimation-Based Methods. In Proceedings of the 2021 11th Smart Grid Conference (SGC), Tabriz, Iran, 7–9 December 2021. [CrossRef]
92. Aruna Gawade, N.S. MITM Attack Prevention Using PUF Authentication in Smart Grid. *Int. J. Adv. Sci. Technol.* **2020**, *29*, 12321–12331.
93. Wlazlo, P.; Sahu, A.; Mao, Z.; Huang, H.; Goulart, A.E.; Davis, K.R.; Zonouz, S.A. Man-in-The-Middle Attacks and Defense in a Power System Cyber-Physical Testbed. *arXiv* **2021**, arXiv:2102.11455.
94. Mohsenian-Rad, A.H.; Leon-Garcia, A. Distributed Internet-Based Load Altering Attacks against Smart Power Grids. *IEEE Trans. Smart Grid* **2011**, *2*, 667–674. [CrossRef]
95. Amini, S.; Pasqualetti, F.; Mohsenian-Rad, H. Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Schemes. *IEEE Trans. Smart Grid* **2018**, *9*, 2862–2872. [CrossRef]
96. Amini, S.; Pasqualetti, F.; Abbaszadeh, M.; Mohsenian-Rad, H. Hierarchical Location Identification of Destabilizing Faults and Attacks in Power Systems: A Frequency-Domain Approach. *IEEE Trans. Smart Grid* **2019**, *10*, 2036–2045. [CrossRef]
97. Gobmaier, T. Measuring Devices for Frequency Measurement. Available online: https://www.mainsfrequency.com/meter.htm (accessed on 5 March 2022).
98. Zhao, C.; Topcu, U.; Low, S.H. Optimal Load Control via Frequency Measurement and Neighborhood Area Communication. *IEEE Trans. Power Syst.* **2013**, *28*, 3576–3587. [CrossRef]
99. Huang, B.; Cardenas, A.A.; Baldick, R. Not Everything is Dark and Gloomy: Power Grid Protections Against IoT Demand Attacks. In Proceedings of the 28th USENIX Security Symposium (USENIX Security 19), Santa Clara, CA, USA, 14–16 August 2019; USENIX Association: Santa Clara, CA, USA, 2019; pp. 1115–1132.
100. 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]
101. Ma, Q.; Xu, Z.; Wang, W.; Lin, L.; Ren, T.; Yang, S.; Li, J. Dynamic load-altering attack detection based on adaptive fading Kalman filter in power systems. *Glob. Energy Interconnect.* **2021**, *4*, 184–192. [CrossRef]
102. Chen, C.; Cui, M.; Fang, X.; Ren, B.; Chen, Y. Load altering attack-tolerant defense strategy for load frequency control system. *Appl. Energy* **2020**, *280*, 116015. [CrossRef]
103. Chakrabarty, S.; Sikdar, B. Detection of Malicious Command Injection Attacks on Phase Shifter Control in Power Systems. *IEEE Trans. Power Syst.* **2021**, *36*, 271–280. [CrossRef]
104. Lin, H.; Kalbarczyk, Z.; Iyer, R.K. Impact of Malicious SCADA Commands on Power Grids' Dynamic Responses. In Proceedings of the 2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Aalborg, Denmark, 29–31 October 2018. [CrossRef]
105. Chakrabarty, S.; Sikdar, B. Detection of Hidden Transformer Tap Change Command Attacks in Transmission Networks. *IEEE Trans. Smart Grid* **2020**, *11*, 5161–5173. [CrossRef]
106. Wang, H.; Li, J.; Zhang, T.; Ying, H.; Han, J.; Ji, X. Malicious Code Detection on Smart Meters -A Side-Channel Based Approach. In Proceedings of the 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chengdu, China, 15–17 March 2019. [CrossRef]
107. Yuan, Y.; Li, Z.; Ren, K. Quantitative Analysis of Load Redistribution Attacks in Power Systems. *IEEE Trans. Parallel Distrib. Syst.* **2012**, *23*, 1731–1738. [CrossRef]
108. Pinceti, A.; Sankar, L.; Kosut, O. Detection and Localization of Load Redistribution Attacks on Large-Scale Systems. *J. Mod. Power Syst. Clean Energy* **2021**, *10*, 361–370. [CrossRef]

109. Pinceti, A.; Sankar, L.; Kosut, O. Load Redistribution Attack Detection using Machine Learning: A Data-Driven Approach. In Proceedings of the 2018 IEEE Power & Energy Society General Meeting (PESGM), Portland, OR, USA, 5–10 August 2018. [CrossRef]
110. Chu, Z.; Kosut, O.; Sankar, L. Detecting load redistribution attacks via support vector models. *IET Smart Grid* **2020**, *3*, 551–560. [CrossRef]
111. PJM. Load Forecast Development Process. Available online: https://www.pjm.com/planning/resource-adequacy-planning/load-forecast-dev-process.aspx (accessed on 5 February 2022).
112. Zhang, J.; Sankar, L. Implementation of unobservable state-preserving topology attacks. In Proceedings of the 2015 North American Power Symposium (NAPS), Charlotte, NC, USA, 4–6 October 2015. [CrossRef]
113. Zhang, J.; Sankar, L. Physical System Consequences of Unobservable State-and-Topology Cyber-Physical Attacks. *IEEE Trans. Smart Grid* **2016**, *7*, 2016–2025. [CrossRef]
114. Kim, J.; Tong, L. On Topology Attack of a Smart Grid: Undetectable Attacks and Countermeasures. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1294–1305. [CrossRef]
115. Li, Z.; Shahidehpour, M.; Alabdulwahab, A.; Abusorrah, A. Bilevel Model for Analyzing Coordinated Cyber-Physical Attacks on Power Systems. *IEEE Trans. Smart Grid* **2016**, *7*, 2260–2272. [CrossRef]
116. Knapp, E.D.; Samani, R. *Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure*; Elsevier: Amsterdam, The Netherlands, 2013. [CrossRef]
117. Mo, Y.; Weerakkody, S.; Sinopoli, B. Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs. *IEEE Control Syst. Mag.* **2015**, *35*, 93–109. [CrossRef]
118. Mo, Y.; Chabukswar, R.; Sinopoli, B. Detecting Integrity Attacks on SCADA Systems. *IEEE Trans. Control. Syst. Technol.* **2014**, *22*, 1396–1407. [CrossRef]
119. Irita, T.; Namerikawa, T. Detection of replay attack on smart grid with code signal and bargaining game. In Proceedings of the 2017 American Control Conference (ACC), Seattle, WA, USA, 24–26 May 2017. [CrossRef]
120. Ma, M.; Zhou, P.; Du, D.; Peng, C.; Fei, M.; AlBuflasa, H.M. Detecting Replay Attacks in Power Systems: A Data-Driven Approach. In *Communications in Computer and Information Science*; Springer: Singapore, 2017; pp. 450–457. [CrossRef]
121. Abdelwahab, A.; Lucia, W.; Youssef, A. Set-Theoretic Control for Active Detection of Replay Attacks with Applications to Smart Grid. In Proceedings of the 2020 IEEE Conference on Control Technology and Applications (CCTA), Montreal, QC, Canada, 24–26 August 2020. [CrossRef]
122. Hossain-McKenzie, S.; Chavez, A.; Jacobs, N.; Jones, C.B.; Summers, A.; Wright, B. Proactive Intrusion Detection and Mitigation System: Case Study on Packet Replay Attacks in Distributed Energy Resource Systems. In Proceedings of the 2021 IEEE Power and Energy Conference at Illinois (PECI), Urbana, IL, USA, 1–2 April 2021; pp. 1–6. [CrossRef]
123. kaspersky. BlackEnergy APT Attacks in Ukraine. Available online: https://www.kaspersky.com/resource-center/threats/blackenergy (accessed on 5 February 2022).
124. Denning, D.E. Stuxnet: What Has Changed? *Future Internet* **2012**, *4*, 672–687. [CrossRef]
125. Zhang, Z.; Gong, S.; Dimitrovski, A.D.; Li, H. Time Synchronization Attack in Smart Grid: Impact and Analysis. *IEEE Trans. Smart Grid* **2013**, *4*, 87–98. [CrossRef]
126. Park, G.; Shim, H.; Lee, C.; Eun, Y.; Johansson, K.H. When adversary encounters uncertain cyber-physical systems: Robust zero-dynamics attack with disclosure resources. In Proceedings of the 2016 IEEE 55th Conference on Decision and Control (CDC), Las Vegas, NV, USA, 12–14 December 2016. [CrossRef]
127. Zhang, Y.; Wang, J.; Liu, J. Attack Identification and Correction for PMU GPS Spoofing in Unbalanced Distribution Systems. *IEEE Trans. Smart Grid* **2020**, *11*, 762–773. [CrossRef]
128. Li, Y.; Yang, S. GPS Spoofing attack detection in smart grids based on improved CapsNet. *China Commun.* **2021**, *18*, 174–186. [CrossRef]
129. Kumari, A.; Patel, M.M.; Shukla, A.; Tanwar, S.; Kumar, N.; Rodrigues, J.J.P.C. ArMor: A Data Analytics Scheme to identify malicious behaviors on Blockchain-based Smart Grid System. In Proceedings of the GLOBECOM 2020—2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020. [CrossRef]
130. Houda, Z.A.E.; Hafid, A.; Khoukhi, L. Blockchain Meets AMI: Towards Secure Advanced Metering Infrastructures. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020. [CrossRef]
131. Bari, A.; Jiang, J.; Saad, W.; Jaekel, A. Challenges in the Smart Grid Applications: An Overview. *Int. J. Distrib. Sens. Netw.* **2014**, *10*, 974682. [CrossRef]
132. Ramanan, P.; Li, D.; Gebraeel, N. Blockchain-Based Decentralized Replay Attack Detection for Large-Scale Power Systems. *IEEE Trans. Syst. Man Cybern. Syst.* **2022**, *52*, 4727–4739. [CrossRef]
133. Samy, S.; Banawan, K.; Azab, M.; Rizk, M. Smart Blockchain-based Control-data Protection Framework for Trustworthy Smart Grid Operations. In Proceedings of the 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 27–30 October 2021; pp. 0963–0969.
134. Samuel, O.; Javaid, N. GarliChain: A privacy preserving system for smart grid consumers using blockchain. *Int. J. Energy Res.* **2021**, 1–17. [CrossRef]
135. Li, M.; Hu, D.; Lal, C.; Conti, M.; Zhang, Z. Blockchain-Enabled Secure Energy Trading With Verifiable Fairness in Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6564–6574. [CrossRef]

136. Reijsbergen, D.; Maw, A.; Dinh, T.T.A.; Li, W.T.; Yuen, C. Securing Smart Grids Through an Incentive Mechanism for Blockchain-Based Data Sharing. In Proceedings of the Twelveth ACM Conference on Data and Application Security and Privacy, Baltimore, MD, USA, 24–27 April 2022. [CrossRef]
137. Liang, G.; Weller, S.R.; Luo, F.; Zhao, J.; Dong, Z.Y. Distributed Blockchain-Based Data Protection Framework for Modern Power Systems Against Cyber Attacks. *IEEE Trans. Smart Grid* **2019**, *10*, 3162–3173. [CrossRef]
138. Dehalwar, V.; Kolhe, M.L.; Deoli, S.; Jhariya, M.K. Blockchain-based trust management and authentication of devices in smart grid. *Clean. Eng. Technol.* **2022**, *8*, 100481. [CrossRef]
139. Poggio, T.; Mhaskar, H.; Rosasco, L.; Miranda, B.; Liao, Q. Why and when can deep-but not shallow-networks avoid the curse of dimensionality: A review. *Int. J. Autom. Comput.* **2017**, *14*, 503–519. [CrossRef]
140. Sawas, A.M.; Khani, H.; Farag, H.E.Z. On the Resiliency of Power and Gas Integration Resources Against Cyber Attacks. *IEEE Trans. Ind. Inform.* **2021**, *17*, 3099–3110. [CrossRef]
141. Albarakati, A.; Robillard, C.; Karanfil, M.; Kassouf, M.; Debbabi, M.; Youssef, A.; Ghafouri, M.; Hadjidj, R. Security Monitoring of IEC 61850 Substations Using IEC 62351-7 Network and System Management. *IEEE Trans. Ind. Inform.* **2022**, *18*, 1641–1653. [CrossRef]
142. Yao, D.; Wen, M.; Liang, X.; Fu, Z.; Zhang, K.; Yang, B. Energy Theft Detection With Energy Privacy Preservation in the Smart Grid. *IEEE Internet Things J.* **2019**, *6*, 7659–7669. [CrossRef]
143. Kwon, S.; Yoo, H.; Shon, T. IEEE 1815.1-Based Power System Security With Bidirectional RNN-Based Network Anomalous Attack Detection for Cyber-Physical System. *IEEE Access* **2020**, *8*, 77572–77586. [CrossRef]
144. Siniosoglou, I.; Radoglou-Grammatikis, P.; Efstathopoulos, G.; Fouliras, P.; Sarigiannidis, P. A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 1137–1151. [CrossRef]
145. He, Z.; Khazaei, J.; Moazeni, F.; Freihaut, J.D. Detection of false data injection attacks leading to line congestions using Neural networks. *Sustain. Cities Soc.* **2022**, *82*, 103861. [CrossRef]
146. Abdulaal, M.J.; Ibrahem, M.I.; Mahmoud, M.M.E.A.; Khalid, J.; Aljohani, A.J.; Milyani, A.H.; Abusorrah, A.M. Real-Time Detection of False Readings in Smart Grid AMI Using Deep and Ensemble Learning. *IEEE Access* **2022**, *10*, 47541–47556. [CrossRef]
147. Lepolesa, L.J.; Achari, S.; Cheng, L. Electricity Theft Detection in Smart Grids Based on Deep Neural Network. *IEEE Access* **2022**, *10*, 39638–39655. [CrossRef]
148. Khan, S.; Aslam, S.; Mustafa, I.; Aslam, S. Short-Term Electricity Price Forecasting by Employing Ensemble Empirical Mode Decomposition and Extreme Learning Machine. *Forecasting* **2021**, *3*, 28. [CrossRef]
149. 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]
150. 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]
151. Acosta, M.R.C.; Ahmed, S.; Garcia, C.E.; Koo, I. Extremely Randomized Trees-Based Scheme for Stealthy Cyber-Attack Detection in Smart Grid Networks. *IEEE Access* **2020**, *8*, 19921–19933. [CrossRef]
152. Ravikumar, G.; Govindarasu, M. Anomaly Detection and Mitigation for Wide-Area Damping Control using Machine Learning. *IEEE Trans. Smart Grid* **2020**. [CrossRef]
153. Singh, V.K.; Govindarasu, M. A Cyber-Physical Anomaly Detection for Wide-Area Protection Using Machine Learning. *IEEE Trans. Smart Grid* **2021**, *12*, 3514–3526. [CrossRef]
154. Cao, J.; Wang, D.; Qu, Z.; Cui, M.; Xu, P.; Xue, K.; Hu, K. A Novel False Data Injection Attack Detection Model of the Cyber-Physical Power System. *IEEE Access* **2020**, *8*, 95109–95125. [CrossRef]
155. Wu, T.; Xue, W.; Wang, H.; Chung, C.Y.; Wang, G.; Peng, J.; Yang, Q. Extreme Learning Machine-Based State Reconstruction for Automatic Attack Filtering in Cyber Physical Power System. *IEEE Trans. Ind. Inform.* **2021**, *17*, 1892–1904. [CrossRef]
156. Aflaki, A.; Gitizadeh, M.; Razavi-Far, R.; Palade, V.; Ghasemi, A.A. A Hybrid Framework for Detecting and Eliminating Cyber-Attacks in Power Grids. *Energies* **2021**, *14*, 5823. [CrossRef]
157. Parizad, A.; Hatziadoniu, C. Cyber-Attack Detection Using Principal Component Analysis and Noisy Clustering Algorithms: A Collaborative Machine Learning-Based Framework. *IEEE Trans. Smart Grid* **2022**. [CrossRef]
158. McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; Arcas, B.A.y. Communication-Efficient Learning of Deep Networks from Decentralized Data. In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, Fort Lauderdale, FL, USA, 20–22 April 2017; Singh, A., Zhu, J., Eds.; Proceedings of Machine Learning Research; PMLR: Fort Lauderdale, FL, USA, 2017; Volume 54, pp. 1273–1282.
159. Su, Z.; Wang, Y.; Luan, T.H.; Zhang, N.; Li, F.; Chen, T.; Cao, H. Secure and Efficient Federated Learning for Smart Grid with Edge-Cloud Collaboration. *IEEE Trans. Ind. Inform.* **2022**, *18*, 1333–1344. [CrossRef]
160. Qammar, A.; Ding, J.; Ning, H. Federated learning attack surface: Taxonomy, cyber defences, challenges, and future directions. *Artif. Intell. Rev.* **2021**, *55*, 3569–3606. [CrossRef]
161. Li, Z.; Sharma, V.; Mohanty, S.P. Preserving Data Privacy via Federated Learning: Challenges and Solutions. *IEEE Consum. Electron. Mag.* **2020**, *9*, 8–16. [CrossRef]
162. Aklilu, Y.T.; Ding, J. Survey on Blockchain for Smart Grid Management, Control, and Operation. *Energies* **2022**, *15*, 193. [CrossRef]

163. Borgaonkar, R.; Tøndel, I.A.; Degefa, M.Z.; Jaatun, M.G. Improving smart grid security through 5G enabled IoT and edge computing. *Concurr. Comput. Pract. Exp.* **2021**, *33*, e6466. [CrossRef]
164. Hossain, N.U.I.; Nagahi, M.; Jaradat, R.; Shah, C.; Buchanan, R.; Hamilton, M. Modeling and assessing cyber resilience of smart grid using Bayesian network-based approach: A system of systems problem. *J. Comput. Des. Eng.* **2020**, *7*, 352–366. [CrossRef]