sustainability

MDPI

Review

Security Risk Modeling in Smart Grid Critical Infrastructures in the Era of Big Data and Artificial Intelligence

Abdellah Chehri [1,*], Issouf Fofana [1] and Xiaomin Yang [2]

[1] Department of Applied Sciences, University of Quebec in Chicoutimi (UQAC), Chicoutimi, QC G7H 2B1, Canada; ifofana@uqac.ca
[2] College of Electronics and Information Engineering, Sichuan University, Chengdu 610064, China; arielyang@scu.edu.cn
* Correspondence: achehri@uqac.ca

Abstract: Smart grids (SG) emerged as a response to the need to modernize the electricity grid. The current security tools are almost perfect when it comes to identifying and preventing known attacks in the smart grid. Still, unfortunately, they do not quite meet the requirements of advanced cybersecurity. Adequate protection against cyber threats requires a whole set of processes and tools. Therefore, a more flexible mechanism is needed to examine data sets holistically and detect otherwise unknown threats. This is possible with big modern data analyses based on deep learning, machine learning, and artificial intelligence. Machine learning, which can rely on adaptive baseline behavior models, effectively detects new, unknown attacks. Combined known and unknown data sets based on predictive analytics and machine intelligence will decisively change the security landscape. This paper identifies the trends, problems, and challenges of cybersecurity in smart grid critical infrastructures in big data and artificial intelligence. We present an overview of the SG with its architectures and functionalities and confirm how technology has configured the modern electricity grid. A qualitative risk assessment method is presented. The most significant contributions to the reliability, safety, and efficiency of the electrical network are described. We expose levels while proposing suitable security countermeasures. Finally, the smart grid's cybersecurity risk assessment methods for supervisory control and data acquisition are presented.

Keywords: smart grid; cybersecurity; machine learning; optimization; deep learning; cybersecurity risks; automated distribution network

check for updates

Citation: Chehri, A.; Fofana, I.; Yang, X. Security Risk Modeling in Smart Grid Critical Infrastructures in the Era of Big Data and Artificial Intelligence. *Sustainability* **2021**, *13*, 3196. https://doi.org/10.3390/su13063196

Academic Editor: J. C. Hernandez

Received: 21 December 2020
Accepted: 3 March 2021
Published: 15 March 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The concept of a "smart and sustainable city" is emerging with two flagship applications worldwide. The first target is to use better energy management—particularly with "smart" electricity grids promoting renewable energies. The second one is to deploy efficient mobility solutions to limit the automobile's use and, thus, limit greenhouse gas emissions. As useful as they are, information and communications technologies (ICT) are not an end in themselves.

A smart and sustainable city is an innovative urban strategy, using information and communications technologies to reduce the city's environmental footprint and improve citizens' quality of life. Indeed, the goal of using ICT is not only to increase the "IQ of the city" but to make it more sustainable and more pleasant to live in. This is a formidable challenge when we know that cities bring together an increasingly large population, expand and become denser with the attendant nuisances that this can imply [1].

The electricity sector is evolving towards a modern and automated distribution network. The demand for more digitized, connected, and integrated operations are growing in all sectors, so electricity companies must ensure a reliable power supply, with an approach based on efficiency and sustainable sources [2–4]. As the electrical grid merges and

becomes "smarter" with the resultant benefits of better connectivity, cybersecurity risks, and threats also increase.

Smart grid technology will allow a better adaptation to the dynamics of renewable energy and distributed generation, providing networks and consumers with more direct access to the benefits associated with these resources. An intelligent system's abilities will allow the easy and straightforward control of the bidirectional flow of electrical energy and facilitate the actions of monitoring, management, and support of resources at the distribution level.

Smart grids are autonomous and improve the effectiveness and efficiency of electrical power management, allowing utilities to optimize existing infrastructure, minimizing the construction of more power plants.

The main objective is to make the system more flexible to accommodate both the centralized renewable generation and all the generation and storage options linked to the distribution system [5–10].

For system security, it will bring about a radical change, both in supply and in the event of disasters, since the decentralization of generation will reduce the number of sensitive targets, such as large power plants.

From the environmental point of view, the modernization of the system will contribute much to the reduction in greenhouse gas emissions by promoting even greater distributed generation (especially concerning micro-generation through clean technologies), as well as the emergence of reliable sites for renewable sources, mainly hydro and solar, by avoiding the problems associated with intermittent supply and reducing the need to invest in a centralized fossil-source generation.

The analysis of threats in smart grid (SG) systems and the model of security threats in embedded systems helps to understand better attackers' weaknesses. For example, based on interactions in formalized incentive structures, the game theory approach allows us to carry out decision processes to address cybersecurity in monitoring and protection. Similarly, control from a coordinated cyber-attack perspective can improve security. In short, energy sector associations manage cybersecurity while maintaining critical power supply functions to ensure the modernized grid's reliability.

However, the most significant contributions to the reliability, safety, and efficiency of the electrical network have taken place in the development of intelligent optimization algorithms, such as genetic algorithms, neural networks, game theory strategies, reinforcement learning, vector support machines, among others. These previous strategies have made it possible to study the interactions in formalized security structures in response to demand in the energy markets. Consequently, modern SG control and monitoring systems have made rapid identification of critical infrastructure elements [11–17].

The International Organization for Standardization defines cybersecurity or cyberspace security as preserving confidentiality, integrity, and information availability in cyberspace. In turn, "cyberspace" is defined as "the complex environment resulting from the interaction of people, software and services on the Internet through technology devices and networks connected to it, which does not exist in any physical form".

In this work, we conduct a comprehensive overview and analysis of smart grid architecture and different security aspects in the era of big data and artificial intelligence. It is also a risk-based cybersecurity framework—a set of industry standards and best practices to help SG operators manage cybersecurity risks.

The paper's structure is as follows: Section 2 explores energy management in smart, sustainable cities. The main security threats in smart grids are given in Section 3. Section 4 provides the security-aware of SG infrastructures in the era of big data and artificial intelligence. A survey on risk modeling techniques is given in Section 5. We summarize the most efficient approach of mitigating cyber-attack risk on smart grid systems in Section 6. Section 7 concludes this survey paper.

2. Energy Management in Smart Sustainable Cities

The implementation of the smart and sustainable city, a complex system, requires new governance involving all the connected actors—local communities, companies, citizens—and a lot of research is required to draw its contours.

The concept of a "smart and sustainable city" is attractive. According to lifestyles and social and environmental issues, information and communication technologies to optimize and develop the city's functioning are indeed auspicious. Cities are implementing digital applications to give themselves a little more "intelligence" all over the world. That said, making a city more digital and smarter is not an end in itself. Information technologies are only one tool to achieve an objective: to make the city more pleasant to live in for its inhabitants, to make it cleaner, more economical, more fluid, and more participatory. In short, the challenge is to make the city more sustainable and livable, which, beyond technology, implies a new organization of its players, relying in particular on the participation of citizens.

The stakes are high. By 2025, around 58% of the world's population (4.6 billion people) will live in an urban area, and this rate will reach 80% for developed countries. By 2050, 75% of the world's population will live in cities, which are denser and more populated.

The challenge of urbanization is considerable: overpopulation, climate change, quality of the environment, access to energy, etc. Agglomerations consume around 65% of available primary energy and account for about 70% of greenhouse gas emissions, mainly due to the supply of energy for lighting, heating, and transport. To respond to these challenges, climate change, and deterioration in air quality, the city of tomorrow will have to structure itself.

Of all the possibilities that exist, energy management is the preferred application today by many cities. The energy issue is decisive, both for its effect on climate change and its impact on cities and citizens' bills. When it comes to energy, the smart city is often identified with the "smart grid". Thanks to smart meters equipped with sensors, it is possible to know the consumption of all buildings—housing, office buildings, etc.—particularly to identify the peak moments of energy consumption at the scale of a district and, ultimately, an entire city. These data make it possible to smooth consumption at peak hours by disconnecting devices and also to give consumers essential information to act on their behavior. This information on consumption, together with the decentralized production of electricity from renewable energies (wind, photovoltaic, cogeneration, geothermal energy, etc.) and electricity storage (mainly in batteries today), still allows for management of the production and use of electricity in an optimized way. Typically, the energy accumulated by photovoltaic panels placed on office buildings can be stored and delivered during the evening—that is, when offices are empty—to homes. Electric vehicles can be called upon to provide electricity during peak periods or serve as a storage system during off-peak hours [18–22].

3. Security Threats in Smart Grids

Smart grids reliability is based on the confidence, security, and availability of control of communication application systems [23].

Big Data processes an enormous number of datasets through computer devices and networks to generate useful information for supporting organizational decision-making. The architecture and framework of Big Data illustrate how hardware, software, networking, and data technologies orchestrate to perform the ultimate goal of this innovative methodology.

One of the sources of vulnerability resulting from integrating ICTs to SG is that all devices pass their data through the public network that is the Internet using the Internet Protocol (IP). However, this protocol has known weaknesses that can facilitate the risks of intrusions or interceptions of data. Yet, they have serious security gaps. Therefore, the safety in smart grids implies the protection and security of information.

The smart grid's major security requirements are the CIA triad (confidentiality, availability, and integrity). Before implementing cybersecurity measures and solutions that ensure safe and reliable operation, it is essential to understand the electrical network's safety objectives and requirements. The main goals and objectives are described below.

- Availability: guarantee access and timely use, and reliable information. Data availability is one of the most critical aspects of smart grids. A loss of availability represents the interruption of access and use of information, which could weaken the management and delivery of energy.
- Integrity: ensuring that information is not altered in a way unauthorized. This policy protects against modification and inappropriate destruction of data, ensuring this non-repudiation and its authenticity.
- Confidentiality: preserve the restriction of access and disclosure of the information. This policy addresses the protection of property of the data ensuring that sensitive data is not disclosed to unauthorized persons, entities, or processes [24].

Cybersecurity threats can be associated with the three major security requirements are discussed in Table 1.

Table 1. Malicious attacks on the smart grid.

According to Threat	Security Objective Affected	Active or Passive	Examples
Interception (when personal unauthorized gets access to data, devices, or components cyber environment)	Confidentiality	Passive (usually cannot be detected but can be prevented with cryptography)	Denial of services (DoS), data traffic monitoring
Modification (when accessing) and modifications are made to data, environmental devices, or components cyber deliberately and illegally)	Integrity	Active (can be detected with cryptography)	Modification of control signals, modification of sensor data, modification of information (by example, energy use)
Interrupt (when data, devices, or components of the cyber environment are destroyed or turned to not available to delay, block, or impair the communication in the smart grid)	Availability	Active (can be detected, but usually not prevented)	Elimination of routing, software modification of deleting data, etc.
Manufacturing (when personnel not authorized inserts objects (for example, data or components) false in the system.	Authenticity	Active (can be detected with cryptography)	Saturation attacks, insertion of false control signals, insert of financial transactions bogus for-profit

The National Institute of Standards and Technology (NIST) recommends individual security requirements specific to the smart grid, including cybersecurity and physical security [25].

As this article focuses on the security communication networks, below are some of the most critical cybersecurity requirements for intelligent electrical power systems based on the study developed in [26].

- Privacy: The smart meters and load management in networks intelligent electricity systems involve the use of patterns of electricity that could reveal private information [16,17,19,27]. For example, malicious users could use consumption patterns to determine how much energy is used in a residence or building and find out if consumers are or are not in them and thus be able to execute attacks. In addition, criminals could use information from these patterns to harm specific consumers. As a result, various privacy concerns must be addressed. Fortunately, the technologies related to privacy are very well developed, and the specific privacy solutions needed will depend on the type of protected communication resource [28].
- Attack detection and rapid response to incidents: The smart network electricity is a communication network that includes excellent coverage. Therefore, it is practically impossible to protect every node on the network. As a result, it is recommended to

perform profile checks, tests consistently, and make comparisons to monitor the state of network traffic to detect and identify abnormal incidents due to attacks [26].

- Continuity of operations: an information system of smart grids must have the ability to continue or resume operations in case of interruption of its normal functioning. The work presented in [26] introduces recommendations on policies and procedures of roles and responsibilities, storage centers alternative methods, alternative command and control methods, alternative control, recovery and reconstitution, and response to failure testing information regarding continuity of smart grid operations.
- Identification, authentication, and access control: The networks of smart electrical devices are made up of millions of devices electronic and intelligent information systems. Therefore, identification and authentication should be essential procedures for verifying a user or device's identity and a prerequisite to access resources in the smart grid's information system. This access control focuses on ensuring that resources are only accessed by staff appropriately and adequately identified. To achieve this, each node on the network must have essential cryptographic functions to perform authentications and data encryption [29].
- Audit and accountability: Periodic audits are used to detect gaps in security services to thoroughly examine smart grids' information system records [30,31]. Registration is required to detect anomalies; with the convergence of traditional electrical systems and information technology, the correct analysis of event information (for example, the power outage is necessary to understand what happened).

4. Security-Aware of SG Infrastructures in Era of Big Data and Artificial Intelligence

SG vulnerabilities are most common in smart meters, devices that interact with electricity supply and demand. This is a function of the geographic location where the meters are installed and the encryption level with which the energy consumption analysis algorithms are encoded [32,33].

Smart grids encompass the integration of information technologies for the electricity grid infrastructure. Consequently, the system's automatic operation allows effective options for both utility operators and clients—the preceding under the precept of guaranteeing the electricity supply's reliability and continuity.

Some supervisory control and data acquisition (SCADA) systems or elements were put in place dozens of years ago and are now impossible to update. Some of them were designed before well-founded cybersecurity principles were settled upon. SCADA system designers would claim that cybersecurity is not a concern since SCADA systems are not connected to the Internet. However, over time, SCADA systems began appearing on the Internet, and often with no cybersecurity. These systems must be replaced by more recent, safer equipment, but this is synonymous with significant investments and, therefore, often postponed.

On larger sites, the control system needs to be protected from attack within the SCADA network. Implementing an additional firewall between the corporate and SCADA network can achieve by imposing more restrictive rules. This will enable authorized service engineers to provide support and manage security, e.g., apply security mitigations, inspect log files, apply updates, etc.

Related studies in communications areas include communication network requirements for the main SG applications in domestic air networks, near air networks (NAN), and comprehensive air networks. For example, Bekara investigated security challenges in SGs based on Internet of Things (IoT). The author defined the primary security services that should be considered [34].

The concept has evolved, and today IoT encompasses many other technologies, including wireless sensor networks, machine-to-machine communications, and others, such as ZigBee, WiFi, NB-IoT, LTE, Bluetooth, among others. In Figure 1, it is possible to appreciate the myriad of information and telecommunications technologies that can operate in an electrical distribution system [35].

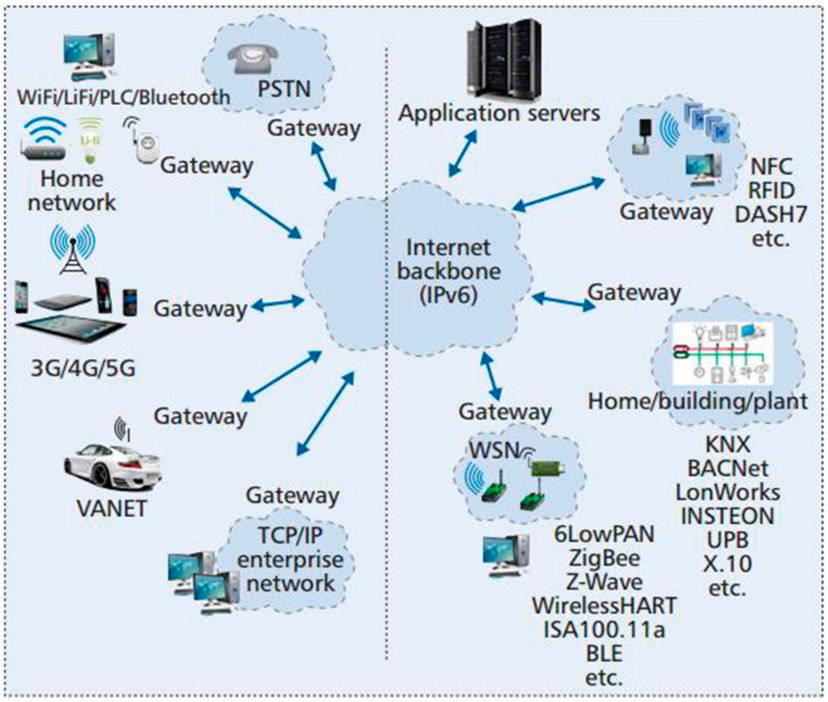

Figure 1. Myriad of information and telecommunications technologies [35].

4.1. The Enormous Potential of Big Data

The most important resource in the world is no longer crude oil, but data—according to *The Economist's* title from 6 May 2017. This lead story expresses the current assessment of big data well. Big data—a term for which there is no generally accepted definition—is pragmatic as a large amount of data, the analysis of which requires the use of tools that go beyond the classic application programs [36]. The acquisition, storage, analysis, maintenance, search, distribution, transmission, visualization, query, update, and data protection are challenges due to the database's size (as shown in Figure 2). There are three general approaches to analyze harmonized data across different sources: pooled data analysis, summary data meta-analysis, and federated data analysis [37–39].

Figure 2. The properties of Big Data are reflected by 5Vs, which are veracity, volume, variety, value, velocity [40].

Thanks to forward-looking algorithms (i.e., prediction of consumption according to the weather, forecasting of production, etc.), the SG has a global vision in real-time or in advance of these energy offers and demands.

The smart grid's strength lies in using this data to automatically adjust the energy flows of the network to supply areas of energy need with electricity primarily from renewable sources.

Electricity distributors are now actively engaged in a double movement towards Big Data—the quantitative explosion of data digital available—and to Open Data—the update free disposal of this data in an open manner, which allows their reuse without technical restriction [40].

4.2. Cybersecurity and Artificial Intelligence

Cybersecurity is one of the many uses of artificial intelligence (AI) [41]. Buzzwords, such as machine learning, natural language processing, and robot-assisted process automation (RPA), are currently primarily associated with digitized production processes [41]. But these technologies have also long been used in cybersecurity. The spam filter, for example, is an excellent example of the application of machine learning that dates back to the early 2000s [42–44]. Of course, the methods have become more refined over time, and the systems now deliver analyses at a much higher level.

Today, the latest developments in artificial intelligence are already making a valuable contribution to improving digital security in the smart grid. The innovations in this area help to defend against a whole range of attack vectors. The five most common use cases are fraud detection, malware detection, intrusion detection, risk assessment, and user behavior analysis. Artificial intelligence is implemented more often than is generally known.

AI delivers insights that allow businesses to quickly understand threats, reducing response times and keeping businesses in compliance with security best practices. Artificial intelligence, 5G, and other technologies are poised to aid with these challenges, but the energy industry must continue to invest in getting ahead of cyberattacks [45]. Another AI application field is the detection and prevention of unauthorized access to network infrastructures (intrusion prevention), be it external or internal. Deep Learning (DL) systems also support user account monitoring. The AI algorithms examine user behavior and can thus detect anomalies—e.g., through different geolocations within a very short time, unusual working and access times, or the use of databases that were previously not or only rarely used [46–48].

On the other hand, machine learning (ML) helps to recognize patterns in data so that machines can learn from experience [49]. By leveraging cyber threat intelligence, smart grid users can respond to problems quickly and confidently [50,51].

The current security tools are almost perfect for identifying and preventing known attacks, but unfortunately, they do not quite meet the requirements of advanced cybersecurity. These solutions offer no protection against new, unknown attacks, zero-day attacks, and low and slow attacks. Therefore, a more flexible mechanism is needed to examine data sets holistically and detect otherwise unknown threats [52–69]. Machine learning, which can rely on adaptive baseline behavior models, is extremely effective in detecting new, unknown attacks: The combination of known and unknown data sets based on predictive analytics and machine intelligence will decisively change the security landscape [70–74]. Table 2 shows how AI can boost cybersecurity in SG.

Table 2. Artificial intelligence (AI) and Cybersecurity.

How AI Can Help in Cybersecurity	References
Automated Detection	[52–56]
Quick Identification Errors	[57]
Secure Authentication	[58–60]
Faster Response Times	[61–64]
Cybersecurity without Errors	[65–68]

5. Survey on Risk Modeling Techniques

To keep pace with these developments and not be helpless in the face of AI-based cyber-attacks, electric utility companies are ultimately almost forced to base their security strategy on similar technologies [75–78]. There are already many effective AI-based security solutions available, especially in endpoint protection. Unlike conventional signature-based protection technologies, these next-generation solutions focus on dynamic behavior analysis techniques and combine these with machine learning and intelligent automation [79–83]. Infections with malicious code are identified here based on their execution behavior within a few seconds and automatically blocked before damage can occur [83]. Machine learning capabilities ensure that the behavior analysis technology is constantly learning and, thanks to the constantly flowing information about threats, is continuously optimized [84].

Cybercriminals are still causing billions in damage using traditional attack methods, and without the use of artificial intelligence, it says a lot about the current state of IT security.

Some of the leading SG research technologies are mentioned in this section. The previous techniques are based on the dynamic integration of electrical engineering developments, energy storage, big data analysis, advances in information, communication technologies (ICT), wireless communication, and machine learning techniques [85–87]. Furthermore, advanced fault management is possible, thanks to the complete coordination of local automation. That is why these sophisticated systems can be used to protect essential consumers from interruptions. In this order of ideas, diagnostic techniques are essential in SG since they must be fault-tolerant [88,89].

5.1. CORAS Method for Security Risk Analysis

A literature review is used in this article to explore various security modeling techniques and their applicability in smart grid security [41]. The CORAS method for security risk analysis was used, as shown in Figure 3.

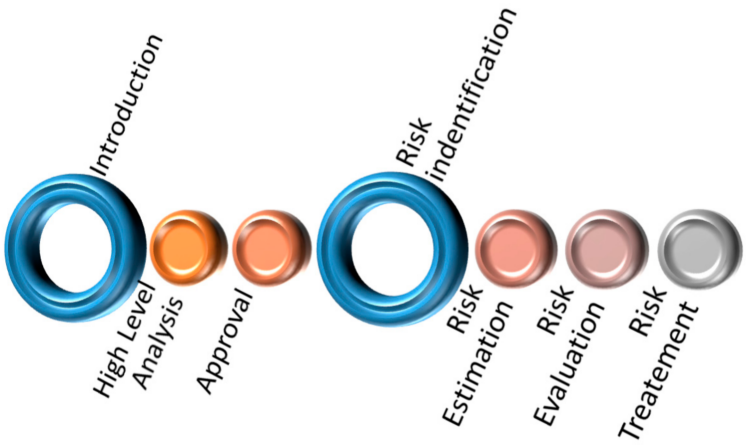

Figure 3. CORAS method for security risk analysis.

The electronic databases IEEEXplore and SpringerLink were used in this literature review. The work consists of a main qualitative study supplemented by a quantitative study. Building a database is not as easy as it sounds to create the comparative databases, and search keywords. Among these keywords, we can quote "attack tree security", "vulnerability analysis", "false data injection attack detection", "malicious behavior detection", "deep learning detection of electricity theft cyber-attacks", "fraud detection", "bow tie security", "anomaly detection method", "smart grids cyber-attack defense", and "CORAS security".

These data were sufficient to create a comparative database and apply high-level quality indicators. Table 3 shows the number of hits each of the keywords returned from IEEEXplore and SpringerLink databases.

Table 3. Classification based on security requirements.

Attacks	References
Switching Attacks	[46–48,51,56,63,66–69,75,77,79,84,85,89–94]
DoS (Denial of Service)	[95–99]
Fraud Detection	[78,96,100]
Cyber Threat Detection	[14,29,96,97,101–104]
Data Integrity	[105–112]
Replay	[113–116]
Packet Dropping	[117–119]
Dynamic Load Altering Attack	[5,27,120–126]
Data Injection Attacks	[47,57,59,75,89,101,107,127–137]
Malicious Software (Malware)	[92,109,113,114,138–144]
Vulnerability Analysis	[80,104,145–147]
Anomaly Detection	[83,148–151]

5.2. Cyber Security Risk Assessment Methods for SCADA Systems

This work has a qualitative approach. It intends to make a reflective analysis based on the documentary review on some methodologies implemented to evaluate cybersecurity risk applied to SCADA (supervisory control and data acquisition) systems for electricity companies. What are the appropriate methods to implement in electricity companies, taking into account vulnerabilities? What are the shortcomings and possibilities for improvement in the current plans?

- Method 1: Analysis, classification, and detection methods of attacks through wireless sensor networks in the smart grid and SCADA systems [152].
- Method 2: Detection of cyberattacks using temporal pattern recognition techniques [153].
- Method 3: A CPI-enabled firewall model for SCADA security in smart grid networks [154].
- Method 4: Combining ensemble methods and social media metrics to improve the accuracy of One Class Support Vector Machine (OCSVM) in intrusion detection in SCADA systems [155].
- Method 5: Unconditional security practical implementation for the IEC 60780-5-101 SCADA protocol [156].
- Method 6: SCADA approach as a service for the interoperability of micro-network platforms. According to [157], in the context of the development of smart grids, this work considered the interoperability of microgrid platforms. Various levels of interoperability were introduced with the respective requirements. The document's main objective was to propose a suitable hybrid cloud-based private SCADA architecture satisfying multiple needs within the interoperability of micro-network platforms while maintaining security constraint conditions. Interoperability between micro-networks will allow research institutions to exchange meaningful information, gain access to the pool of shared resources, and eventually, locally or remotely, borrow associated infrastructure for research activities.
- Method 7: Simulation platform for cybersecurity and critical infrastructure vulnerability analysis [158].
- Method 8: Pre-distribution key scheme with joint license support for SCADA systems [159].
- Method 9: Development of a secure and attack-resistant SCADA system using Wireless Sensor Network (WSN), Mobile Ad hoc NETwork (MANET), and the Internet [160].
- Method 10: Cascading dynamics vulnerability analysis in smart grids under load redistribution attacks [161].
- Method 11: Ensure operations in the industrial control system based on the SCADA-IoT platform using deep belief [162].
- Method 12: An improved algorithm based on optimization for intrusion detection in the SCADA network [163].

The list of the risk assessment methods described in this subsection is summarized in Table 4.

Table 4. Cyber security risk assessment methods for supervisory control and data acquisition (SCADA) systems.

Method	References
Analysis, classification, and detection methods of attacks through wireless sensor networks	[152]
Detection of cyberattacks using temporal pattern recognition techniques	[153]
CPI-enabled firewall model for SCADA security in smart grid networks	[154]
Combining ensemble methods and social media metrics to improve the accuracy of OCSVM in intrusion detection in SCADA systems	[155]
Vulnerability Analysis	[156]
Data Integrity for cloud-based private SCADA architecture	[157]
Simulation and Malicious Software (Malware)	[158]
Replay and pre-distribution key scheme	[159]
Packet Dropping and attack-resistant SCADA system	[160]
Dynamic Load Altering Attack	[161]
Data Injection Attacks using using deep belief	[162]
Anomaly Detection and optimization for intrusion detection	[163]

6. Mitigating the Risk of Cyber Attack on Smart Grid Systems

Protecting against today's cyber threats requires greater collaboration between engineers, IT managers, consumers, and security managers, who must share their knowledge to identify potential problems and attacks that affect their smart grid systems. Utilities need to consider how cybersecurity strategies will evolve. It is about staying current against known threats in a planned and iterative way. Having a good defense against cyber-attacks is an ongoing process and requires constant effort. Electricity companies must implement a complete program that integrates a good organization and adequate processes.

The traditional tiered approach to cybersecurity can only prevent and detect the less elaborate threats. In the meantime, modern cyber-attacks are carefully designed to bypass standard security controls by learning detection rules. In addition, traditional controls may not adequately counter insider threats, a form of insidious attack launched by those with legitimate access.

By leveraging AI and advanced big data analytics, cybersecurity technologies can generate predictive and actionable insights that will help you make better cybersecurity decisions and protect your smart grid against threats. They can also help the electric utility detect and counter threats faster by monitoring the cyber environment at speed and with a precision level that only machines can.

Artificial intelligence technologies are already integrated into tools, such as antivirus, EDR (endpoint detection and response) solutions, firewalls, data loss prevention, etc., that automatically respond to attacks by filtering malicious traffic. Vulnerability management has become a point of tension for operational teams due to the constant increase in the number of known vulnerabilities, difficulties in assessing the real risks induced, and prioritizing and automating patches' deployment. Indeed, of the thousands of vulnerabilities published each year, only a fraction is used by attackers. Besides, some systems are protected by perimeter defenses.

This complexity is driving vulnerability management tool vendors to integrate AI technologies into their solutions. The objective of AI applied to vulnerability management is to improve the discovery of active equipment, the scanning of vulnerabilities, the determination of associated risks connected with intelligence on the threat, the prioritization, and deployment of patches.

Establishing and maintaining a robust and adequately implemented cybersecurity awareness program for SG, several approaches (as shown in Figure 4) must be followed:

- Secured Remote Access: The mere protection by the combination of password and user name is by no means sufficient here. Encrypted connections, for example, via

VPN (virtual private network), are a better choice here [82]. These considerations already show that there is no universal security solution that fits all companies and electric utilities but that the corresponding measures must always be tailored to the operational requirements. This is the only way to guarantee meaningful protection.

- Traffic Control: The first step is to control the data traffic, for example, through a firewall, which ideally not only separates the internal IT systems from the Internet but very precisely regulates which IT systems are allowed to communicate with which Operational technology (OT) systems, and also which protocols they are allowed to use for this. If, for example, an IT system should only communicate with an OT system via an HTTPS connection, it makes sense to limit communication to precisely this protocol [164–166]. This means that attacks based on the SMB (server message block) protocol, for example, are no longer possible.
- Conduct a risk assessment: The first step is to conduct a comprehensive risk assessment based on internal and external threats [167]. By doing so, specialists will understand their most vulnerable points and define security policies and risk migration [168].
- Design a security policy and processes: The cybersecurity policy of a power company provides a set of rules to follow. The purpose of an electric company's policy is to inform employees, suppliers, and other authorized users of their obligations concerning the protection of technological assets and information [169] and security policy violation [170]. One of the keys to maintaining a practical base is conducting a review once or twice a year.
- Execute projects that implement the risk mitigation plan: It is crucial to select a cybersecurity technology based on international standards [171,172].
- The anomaly detection by deep packet inspection, i.e., the "deep look" into the data communication, not only brings a considerable security advantage in the electrical industry but can also significantly increase productivity. In this way, new communication protocols, or even measured values that do not move within a defined framework, are recognized in real-time. This means that an attack or a creeping error can be reacted to very quickly before damage occurs. With this approach—after a learning phase—the normal behavior of the system is known. Anything that deviates from it in any way is recognized as an anomaly and triggers an alarm. The reasons for such a deviation can be varied, for example, a defective sensor, a new notebook belonging to a service employee, or an attack by a virus.

Figure 4. Mitigating the risk of cyber attack on smart grid systems.

7. Conclusions

The smart grid's basic idea is not enough when embarking on this complex system. Even with the available experiences and technologies, the ideal network's search is an investment based on time, money, and research. With the great efforts put forth for SG research, the power sector players pursue the energy revolution that humanity longs for.

The smart grid becomes more complex when environments involve numerous devices and increasing connectivity to other networks, including the Internet. For such systems, it is important to understand and comprehend the cyber elements and the implications of the integrated state of the environment. Furthermore, the diversity of the hardware and software in the SG sensors provides strong market competition, but this diversity is also a security issue in that there is no single security architect overseeing the entire "system" of the SG. Cybersecurity experts agree that standards alone will not provide the appropriate level of security.

Will artificial intelligence be the next step in our evolution? Although it is still in its infancy, AI is already changing the way we do things. Artificial intelligence, such as deep learning, are key topics that have been driving new technologies. AI technologies have great potential, especially when it comes to defending against cyber-attacks.

Despite existing guidelines and frameworks, designing and managing security for SG remains difficult. This paper identifies the trends, problems, and challenges of cybersecurity in smart grid critical infrastructures in big data and artificial intelligence. An extensive state-of-art analysis was completed—some specific guidelines for achieving cybersecurity awareness program for SG were discussed.

Author Contributions: Investigation, A.C.; writing—original draft preparation, A.C., I.F., X.Y.; writing—review and editing A.C., I.F., X.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Klaimi, J.; Rahim-Amoud, R.; Merghem-Boulahia, L.; Jrad, A. A novel loss-based energy management approach for smart grids using multi-agent systems and intelligent storage systems. *Sustain. Cities Soc.* **2018**, *39*, 344–357. [CrossRef]
2. Marah, R.; El Hibaoui, A. Algorithms for Smart Grid management. *Sustain. Cities Soc.* **2018**, *38*, 627–635. [CrossRef]
3. Qureshi, K.N.; Hussain, R.; Jeon, G. A Distributed Software Defined Networking Model to Improve the Scalability and Quality of Services for Flexible Green Energy Internet for Smart Grid Systems. *Comput. Electr. Eng.* **2020**, *84*, 106634. [CrossRef]
4. Manbachi, M.; Farhangi, H.; Palizban, A.; Arzanpour, S. Smart grid adaptive volt-VAR optimization: Challenges for sustainable future grids. *Sustain. Cities Soc.* **2017**, *28*, 242–255. [CrossRef]
5. Chakraborty, N.; Mondal, A.; Mondal, S. Efficient Load Control Based Demand Side Management Schemes towards a Smart Energy Grid System. *Sustain. Cities Soc.* **2020**, *59*, 102175. [CrossRef]
6. Gandhi, I.; Ravi, L.; Vijayakumar, V.; Subramaniyaswamy, V. Improving security for wind energy systems in smart grid applications using digital protection technique. *Sustain. Cities Soc.* **2020**, *60*, 102265.
7. Chehri, A.; Mouftah, H.T. Service-oriented architecture for smart building energy management. In Proceedings of the 2013 IEEE International Conference on Communications (ICC), Budapest, Hungary, 9–13 June 2013; pp. 4099–4103.
8. Chehri, A.; Mouftah, H.T. FEMAN: Fuzzy-based energy management system for green houses using hybrid grid solar power. *J. Renew. Energy* **2013**, *2013*, 785636. [CrossRef]
9. Smart Grid Coordination Group. *Smart Grid Reference Architecture*; CEN-CENELECETSI; Smart Grid Coordination Group: Paris, France, 2012.
10. Neureiter, C.; Uslar, M.; Engel, D.; Lastro, G. A standards-based approach for domain specific modelling of smart grid system architecture. In Proceedings of the 11th International Conference on System of Systems Engineering, Kongsberg, Norway, 12–16 June 2016; pp. 12–16.
11. Ferreira, A.; Leitão, P.; Vrba, P. Challenges of ICT and artificial intelligence in smart grids. In Proceedings of the IEEE International Workshop on Intelligent Energy Systems (IWIES), San Diego, CA, USA, 8 October 2014; pp. 6–11.
12. Specht, M.; Rosinger, C. Standards in the electro mobility domain—vehicle 2 grid. In *Standardization in Smart Grids*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 163–177.
13. Uslar, M.; Specht, M.; Dänekas, C.; Trefke, J.; Rohjans, S.; González, J.M.; Rosinger, C.; Bleiker, R. *Standardization in Smart Grid*; Springer: Berlin/Heidelberg, Germany, 2013.

14. Ghansah, I. *Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks*; CEC-500-2012-047; California Energy Commission, PIER Energy-Related Environmental Research Program: Sacramento, CA, USA, 2009.
15. McDaniel, P.; McLaughlin, S. Security and privacy challenges in the smart grid. *IEEE Secur. Priv. Mag.* **2009**, *7*, 75–77. [CrossRef]
16. Karnouskos, S.; Terzidis, O.; Karnouskos, P. An advanced metering infrastructure for future energy networks. In *New Technologies, Mobility and Security*; Springer: Dordrecht, The Netherlands, 2007; pp. 597–606.
17. Depuru, S.S.; Wang, L.; Devabhaktuni, V.; Gudi, N. Smart meters for power grid: Challenges, issues, advantages and status. *Renew. Sustain. Energy Rev.* **2011**, *15*, 2736–2742. [CrossRef]
18. Shipman, C.M.; Hopkinson, K.M.; Lopez, J. Con-Resistant Trust for Improved Reliability in a Smart-Grid Special Protection System. *IEEE Trans. Power Deliv.* **2014**, *30*, 455–462. [CrossRef]
19. Nordell, D.E. Terms of Protection: The Many Faces of Smart Grid Security. *IEEE Power Energy Mag.* **2012**, *10*, 18–23. [CrossRef]
20. Khurana, H.; Hadley, M.; Lu, N.; Frincke, D.A. Smart-grid security issues. *IEEE Secur. Priv.* **2010**, *8*, 81–85. [CrossRef]
21. Rossebø, J.E.Y.; Wolthuis, R.; Fransen, F.; Björkman, G.; Medeiros, N. An Enhanced Risk-Assessment Methodology for Smart Grids. *Computer* **2017**, *50*, 62–71. [CrossRef]
22. Dechesne, F.; Hadziosmanovic, D.; Pieters, W. Experimenting with Incentives: Security in Pilots for Future Grids. *IEEE Secur. Priv.* **2014**, *12*, 59–66. [CrossRef]
23. Guo, L.; Dong, M.; Ota, K.; Wu, J.; Li, J. Event-oriented dynamic security service for demand response in smart grid employing mobile networks. *China Commun.* **2015**, *12*, 63–75. [CrossRef]
24. 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]
25. Greer, C.; Wollman, D.A.; Prochaska, D.E.; Boynton, P.A.; Mazer, J.A.; Nguyen, C.T.; FitzPatrick, G.J.; Nelson, T.L.; Koepke, G.H.; Hefner, A.R., Jr.; et al. *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0*; NIST: Gaithersburg, MD, USA, 2014.
26. The Smart Grid Interoperability Panel—Cyber Security Working Group. Available online: http://dx.doi.org/10.6028/NIST.IR.7628r1 (accessed on 9 March 2021).
27. Kalogridis, G.; Efthymiou, C.; Denic, S.Z.; Lewis, T.A.; Cepeda, R. Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures. In Proceedings of the 2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA, 4–6 October 2010; pp. 232–237.
28. Yadav, D.; Mahajan, A.R. Smart Grid Cyber Security and Risk Assessment: An Overview. *Int. J. Sci. Eng. Technol. Res.* **2015**, *4*, 3078–3085.
29. Chin, W.; Li, W.; Chen, H. Energy Big Data Security Threats in IoT-Based Smart Grid Communications. *IEEE Commun. Mag.* **2017**, *55*, 70–75. [CrossRef]
30. Li, T.; Ren, J.; Tang, X. Secure wireless monitoring and control systems for smart grid and smart home. *IEEE Wirel. Commun.* **2012**, *19*, 66–73.
31. He, D.; Chan, S.; Guizani, M. Win-Win Security Approaches for Smart Grid Communications Networks. *IEEE Netw.* **2017**, *31*, 122–128. [CrossRef]
32. Ashok, A.; Hahn, A.; Govindarasu, M. Cyber-physical security of Wide-Area Monitoring, Protection and Control in a smart grid environment. *J. Adv. Res.* **2014**, *5*, 481–489. [CrossRef] [PubMed]
33. Avelar, E.; Marques, L.; dos Passos, D.; Macedo, R.; Dias, K.; Nogueira, M. Interoperability issues on heterogeneous wireless communication for smart cities. *Comput. Commun.* **2015**, *58*, 4–15. [CrossRef]
34. Bekara, C. Security issues and challenges for the IoT-based smart grid. *Procedia Comput. Sci.* **2014**, *34*, 532–537. [CrossRef]
35. Meddeb, A. Internet of things standards: Who stands out from the crowd? *IEEE Commun. Mag.* **2016**, *54*, 40–47. [CrossRef]
36. Soundararajan, O.M.; Jenifer, Y.; Dhivya, S.; Rajagopal, T.K.P. Data Security and Privacy in Cloud Using RC6 and SHA Algorithms. *Netw. Commun. Eng.* **2014**, *6*, 202–205.
37. Kolomvatsos, K.; Anagnostopoulos, C.; Hadjiefthymiades, S. An Efficient Time Optimized Scheme for Progressive Analytics in Big Data. *Big Data Res.* **2015**, *2*, 155–165. [CrossRef]
38. Katal, A.; Wazid, M.; Goudar, R.H. Big data: Issues, challenges, tools and Good practices. In Proceedings of the Sixth International Conference on Contemporary Computing, Noida, India, 8–10 August 2013; pp. 404–409.
39. Wang, W.; Lu, Z. Cyber security in the Smart Grid: Survey and challenges. *Int. J. Comput. Telecommun. Netw.* **2013**, *57*, 1344–1371. [CrossRef]
40. Tsai, C.W.; Lai, C.F.; Chao, H.C.; Vasilakos, A.V. Big data analytics: A survey. *J. Big Data* **2015**, *2*, 1–32. [CrossRef]
41. Avevor, W.E. Security of the Smart Grid. Master's Thesis, NTNU, Trondheim, Norway, 2018.
42. Dada, E.G.; Bassi, J.S.; Chiroma, H.; Abdulhamid, S.M.; Adetunmbi, A.O.; Ajibuwa, O.E. Machine learning for email spam filtering: Review, approaches and open research problems. *Heliyon* **2019**, *5*, e01802. [CrossRef]
43. Lueg, C.P. From spam filtering to information retrieval and back: Seeking conceptual foundations for spam filtering. *IEEE Proc. Assoc. Inf. Sci. Technol.* **2005**, *42*. [CrossRef]
44. Wang, X.L. learning to classify email: A survey. *IEEE Int. Conf. Mach. Learn. Cybern.* **2005**, *9*, 5716–5719.
45. Ali, A.B.M.S.; Azad, S.; Khorshed, T. Securing the Smart Grid: A Machine Learning Approach. In *Smart Grids*; Green Energy and Technology; Ali, A., Ed.; Springer: London, UK, 2013.

46. Kurt, M.N.; Ogundijo, O.; Li, C.; Wang, X. Online Cyber-Attack Detection in Smart Grid: A Reinforcement Learning Approach. *IEEE Trans. Smart Grid* **2019**, *10*, 5174–5185. [CrossRef]
47. Wei, J.; Mendis, G.J. A deep learning-based cyber-physical strategy to mitigate false data injection attack in smart grids. In Proceedings of the Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG), Vienna, Austria, 12 April 2016; pp. 1–6.
48. Moslemi, R.; Mesbahi, A.; Velni, J.M. A Fast, Decentralized Covariance Selection-Based Approach to Detect Cyber Attacks in Smart Grids. *IEEE Trans. Smart Grid* **2018**, *9*, 4930–4941. [CrossRef]
49. Ahmed, S.; Lee, Y.; Hyun, S.; Koo, I. Feature Selection–Based Detection of Covert Cyber Deception Assaults in Smart Grid Communications Networks Using Machine Learning. *IEEE Access* **2018**, *6*, 27518–27529. [CrossRef]
50. Zhang, Y.; Wang, L.; Sun, W.; Green, R.C.; Alam, M. Artificial immune system-based intrusion detection in a distributed hierarchical network architecture of smart grid. In Proceedings of the IEEE Power and Energy Society General Meeting, Detroit, MI, USA, 24–28 July 2011; pp. 1–8.
51. Ahmadian, S.; Malki, H.; Han, Z. Cyber Attacks on Smart Energy Grids Using Generative Adverserial Networks. In Proceedings of the 2018 IEEE Global Conference on Signal and Information Processing, Anaheim, CA, USA, 26–29 November 2018.
52. Li, X.; Ma, J.; Zhu, Y.; Liu, Y. Extraction of Abnormal Points from On-line Operation Data of Intelligent Meter Based on LSTM. In Proceedings of the IEEE 9th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), Suzhou, China, 29 July–2 August 2019.
53. Moradi, J.; Shahinzadeh, H.; Nafisi, H.; Marzband, M.; Gharehpetian, G.B. Attributes of Big Data Analytics for Data-Driven Decision Making in Cyber-Physical Power Systems. In Proceedings of the 14th International Conference on Protection and Automation of Power Systems (IPAPS), Tehran, Iran, 31 December 2019–1 January 2020; pp. 83–92.
54. Lin, G.; Liu, S.; Wang, Y. Component Model of Grid Cyber Physical Systems Based on Finite Automata. In Proceedings of the IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chengdu, China, 20–22 December 2019; pp. 2252–2256.
55. Yang, C.; Dubinin, V.; Vyatkin, V. Automatic Generation of Control Flow from Requirements for Distributed Smart Grid Automation Control. *IEEE Trans. Ind. Inf.* **2020**, *16*, 403–413. [CrossRef]
56. Falco, G.; Viswanathan, A.; Caldera, C.; Shrobe, H. A Master Attack Methodology for an AI-Based Automated Attack Planner for Smart Cities. *IEEE Access* **2018**, *6*, 48360–48373. [CrossRef]
57. Alves, H.d.N.; Bretas, N.G.; Bretas, A.S.; Matthews, B. Smart Grids False Data Injection Identification: A Deep Learning Approach. In Proceedings of the IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), Bucharest, Romania, 29 September–2 October 2019; pp. 1–5.
58. Zhang, Y.; Yan, J. Domain-Adversarial Transfer Learning for Robust Intrusion Detection in the Smart Grid. In Proceedings of the IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (Smart Grid Comm), Beijing, China, 21–23 October 2019; pp. 1–6.
59. Nawaz, R.; Shahid, M.A.; Qureshi, I.M.; Mehmood, M.H. Machine learning based false data injection in smart grid. In Proceedings of the 1st International Conference on Power, Energy and Smart Grid, Azad Kashmir, Pakistan, 12–13 April 2018; pp. 1–6.
60. Kaygusuz, C.; Babun, L.; Aksu, H.; Uluagac, A.S. Detection of Compromised Smart Grid Devices with Machine Learning and Convolution Techniques. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, KS, USA, 20–24 May 2018; pp. 1–6.
61. Barati, M. Faster than Real-time Prediction of Disruptions in Power Grids using PMU: Gated Recurrent Unit Approach. In Proceedings of the 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 17–20 February 2019; pp. 1–5.
62. Yang, X.; He, X.; Lin, J.; Yu, W.; Yang, Q. A novel microgrid based resilient Demand Response scheme in smart grid. In Proceedings of the 2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Shanghai, China, 30 May–1 June 2016; pp. 337–342.
63. Lou, X.; Tran, C.; Yau, D.K.; Tan, R.; Ng, H.; Fu, T.Z.; Winslett, M. Learning-Based Time Delay Attack Characterization for Cyber-Physical Systems. In Proceedings of the 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Beijing, China, 21–23 October 2019; pp. 1–6.
64. Ferragut, E.M.; Laska, J.; Olama, M.M.; Ozmen, O. Real-Time Cyber-Physical False Data Attack Detection in Smart Grids Using Neural Networks. In Proceedings of the International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 14–16 December 2017; pp. 1–6.
65. Talei, H.; Essaaidi, M.; Benhaddou, D. An End to End Real Time Architecture for Analyzing and Clustering Time Series Data: Case of an Energy Management System. In Proceedings of the 2018 6th International Renewable and Sustainable Energy Conference (IRSEC), Rabat, Morocco, 5–8 December 2018; pp. 1–7.
66. Wang, H.; Ruan, J.; Wang, G.; Zhou, B.; Liu, Y.; Fu, X.; Peng, J. Deep Learning-Based Interval State Estimation of AC Smart Grids Against Sparse Cyber Attacks. *IEEE Trans. Ind. Inf.* **2018**, *14*, 4766–4778. [CrossRef]
67. Hu, C.; Yan, J.; Wang, C. Advanced Cyber-Physical Attack Classification with Extreme Gradient Boosting for Smart Transmission Grids. In Proceedings of the IEEE Power & Energy Society General Meeting (PESGM), Atlanta, GA, USA, 4–8 August 2019; pp. 1–5.

68. Gunduz, M.Z.; Das, R. Analysis of cyber-attacks on smart grid applications. In Proceedings of the International Conference on Artificial Intelligence and Data Processing (IDAP), Malatya, Turkey, 28–30 September 2018; pp. 1–5.
69. Chen, X.; Zhang, L.; Liu, Y.; Tang, C. Ensemble learning methods for power system cyber-attack detection. In Proceedings of the IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), Chengdu, China, 20–22 April 2018; pp. 613–616.
70. Hossain, E.; Khan, I.; Un-Noor, F.; Sikander, S.S.; Sunny, M.S.H. Application of Big Data and Machine Learning in Smart Grid, and Associated Security Concerns: A Review. *IEEE Access* **2019**, *7*, 13960–13988. [CrossRef]
71. Wu, J.; Ota, K.; Dong, M.; Li, J.; Wang, H. Big Data Analysis-Based Security Situational Awareness for Smart Grid. *IEEE Tran. Big Data* **2018**, *4*, 408–417. [CrossRef]
72. Vijayanand, R.; Devaraj, D.; Kannapiran, B. A Novel Deep Learning Based Intrusion Detection System for Smart Meter Communication Network. In Proceedings of the IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), Tamilnadu, India, 11–13 April 2019; pp. 1–3.
73. Dogaru, D.I.; Dumitrache, I. Cyber Security of Smart Grids in the Context of Big Data and Machine Learning. In Proceedings of the 22nd International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, 28–30 May 2019; pp. 61–67.
74. Singh, S.; Yassine, A.; Benlamri, R. Towards Hybrid Energy Consumption Prediction in Smart Grids with Machine Learning. In Proceedings of the 4th International Conference on Big Data Innovations and Applications (Innovate-Data), Barcelona, Spain, 6–8 August 2018; pp. 44–50.
75. Wang, Y.; Amin, M.M.; Fu, J.; Moussa, H.B. A Novel Data Analytical Approach for False Data Injection Cyber-Physical Attack Mitigation in Smart Grids. *IEEE Access* **2017**, *5*, 26022–26033. [CrossRef]
76. Nabil, M.; Mahmoud, M.; Ismail, M.; Serpedin, E. Deep Recurrent Electricity Theft Detection in AMI Networks with Evolutionary Hyper-Parameter Tuning. In Proceedings of the International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Atlanta, GA, USA, 14–17 July 2019; pp. 1002–1008.
77. Oozeer, M.I.; Haykin, S. Cognitive Risk Control for Mitigating Cyber-Attack in Smart Grid. *IEEE Access* **2019**, *7*, 125806–125826. [CrossRef]
78. Jakaria, A.H.M.; Rahman, M.A.; Hasan, M.G.M.M. Safety Analysis of AMI Networks through Smart Fraud Detection. In Proceedings of the IEEE Conference on Communications and Network Security (CNS), Washington, DC, USA, 10–12 June 2019; pp. 1–7.
79. Yeboah-Ofori, A.; Islam, S.; Brimicombe, A. Detecting Cyber Supply Chain Attacks on Cyber Physical Systems Using Bayesian Belief Network. In Proceedings of the 2019 International Conference on Cyber Security and Internet of Things (ICSIoT), Accra, Ghana, 29–31 May 2019; pp. 37–42.
80. Jiang, H.; Wang, Z.; He, H. An Evolutionary Computation Approach for Smart Grid Cascading Failure Vulnerability Analysis. In Proceedings of the IEEE Symposium Series on Computational Intelligence (SSCI), Xiamen, China, 6–9 December 2019; pp. 332–338.
81. Balduccini, M.; Griffor, E.; Huth, M.; Vishik, C.; Wollman, D.; Kamongi, P. Decision Support for Smart Grid: Using Reasoning to Contextualize Complex Decision Making. In Proceedings of the 2019 7th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), Montreal, QC, Canada, 15–18 April 2019.
82. Seo, S.; Ding, X.; Bertino, E. Encryption key management for secure communication in smart advanced metering infrastructures. In Proceedings of the 2013 IEEE International Conference on Smart Grid Communications (SmartGridComm), Vancouver, BC, Canada, 21–24 October 2013; pp. 498–503.
83. Noureen, S.S.; Bayne, S.B.; Shaffer, E.; Porschet, D.; Berman, M. Anomaly Detection in Cyber-Physical System using Logistic Regression Analysis. In Proceedings of the 2019 IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, 7–8 February 2019; pp. 1–6.
84. 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]
85. Cao, L.; Jiang, X.; Zhao, Y.; Wang, S.; You, D.; Xu, X. A Survey of Network Attacks on Cyber-Physical Systems. *IEEE Access* **2020**, *8*, 44219–44227. [CrossRef]
86. Hussain, S.; Alammari, R.; Iqbal, A.; Shikfa, A. Application of artificial intelligence in electrical power systems. In Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, 2–5 February 2020; pp. 13–17.
87. Karimipour, H.; Dehghantanha, A.; Parizi, R.M.; Choo, K.R.; Leung, H. A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-Scale Smart Grids. *IEEE Access* **2019**, *7*, 80778–80788. [CrossRef]
88. Zhang, Y.; Krishnan, V.V.; Pi, J.; Kaur, K.; Srivastava, A.; Hahn, A.; Suresh, S. Cyber Physical Security Analytics for Transactive Energy Systems. *IEEE Trans. Smart Grid* **2020**, *11*, 931–941. [CrossRef]
89. Wei, F.; Wan, Z.; He, H. Cyber-Attack Recovery Strategy for Smart Grid Based on Deep Reinforcement Learning. *IEEE Trans. Smart Grid* **2020**, *11*, 2476–2486. [CrossRef]
90. Den Braber, F.; Brændeland, G.; Dahl, H.E.I.; Engan, I.; Hogganvik, I.; Lund, M.S.; Solhaug, B.; Stølen, K.; Vraalsen, F. The CORAS model-based method for security risk analysis. *SINTEF Oslo* **2006**, *12*, 15–32.

91. Karbouj, H.; Maity, S. On using TCBR against cyber switching attacks on smart grids. In Proceedings of the IEEE PES Innovative Smart Grid Technologies Conference Europe, Ljubljana, Slovenia, 9–12 October 2016; pp. 665–669.
92. He, H.; Yan, J. Cyber-physical attacks and defences in the smart grid: A survey. *IET Cyber Phys. Syst. Theory Appl.* **2016**, *1*, 13–27. [CrossRef]
93. Farraj, A.; Hammad, E.; Daoud, A.A.; Kundur, D. A Game-Theoretic Analysis of Cyber Switching Attacks and Mitigation in Smart Grid Systems. *IEEE Trans. Smart Grid* **2016**, *7*, 1846–1855. [CrossRef]
94. Farraj, A.; Kundur, D. On using energy storage systems in switching attacks that destabilize smart grid systems. In Proceedings of the 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 18–20 February 2015; pp. 1–5.
95. Ansilla, J.D.; Vasudevan, N.; JayachandraBensam, J.; Anunciya, J.D. Data security in Smart Grid with hardware implementation against DoS attacks. In Proceedings of the 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015], Nagercoil, India, 19–20 March 2015; pp. 1–7. [CrossRef]
96. Wood, P.; Bagchi, S.; Hussain, A. Profiting from attacks on real-time price communications in smart grids. In Proceedings of the 9th International Conference on Communication Systems and Networks, COMSNETS 2017, Bengaluru, India, 4–8 January 2017; pp. 158–165. [CrossRef]
97. Imran, M.; Khan, F.A.; Abbas, H.; Iftikhar, M. Detection and Prevention of Black Hole Attacks in Mobile Ad hoc Networks. 2014. Available online: https://link.springer.com/chapter/10.1007/978-3-662-46338-3_10 (accessed on 14 March 2021). [CrossRef]
98. Kumar, R.J.; Sikdar, B. Efficient Detection of False Data Injection Attacks on AC State Estimation in Smart Grids. In Proceedings of the 2017 IEEE Conference on Communications and Network Security (CNS), Las Vegas, NV, USA, 9–11 October 2017; pp. 411–415.
99. Kurt, M.N.; Yilmaz, Y.; Wang, X. Distributed Quickest Detection of Cyber-Attacks in Smart Grid. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2015–2030. [CrossRef]
100. Amara korba, A.; El Islem karabadji, N. Smart Grid Energy Fraud Detection Using SVM. In Proceedings of the 2019 International Conference on Networking and Advanced Systems (ICNAS), Annaba, Algeria, 26–27 June 2019.
101. 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.
102. Yan, J.; Tang, B.; He, H. Detection of false data attacks in smart grid with supervised learning. In Proceedings of the 2016 International Joint Conference on Neural Networks (IJCNN), Vancouver, BC, Canada, 24–29 July 2016; pp. 1395–1402.
103. Li, B.; Lu, R.; Wang, W.; Choo, K.K.R. DDOA: A Dirichlet-Based Detection Scheme for Opportunistic Attacks in Smart Grid Cyber-Physical System. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 2415–2425. [CrossRef]
104. Yan, J.; Tang, Y.; Zhu, Y.; He, H.; Sun, Y. Smart grid vulnerability under cascade-based sequential line-switching attacks. In Proceedings of the 2015 IEEE Global Communications Conference, GLOBECOM, San Diego, CA, USA, 6–10 December 2015.
105. Yang, X.; Zhang, X.; Lin, J.; Yu, W.; Fu, X.; Zhao, W. Data integrity attacks against the distributed real-time pricing in the smart grid. In Proceedings of the 2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC), Las Vegas, NV, USA, 9–11 December 2016; pp. 1–8.
106. Khanna, K.; Panigrahi, B.K.; Joshi, A. Data integrity attack in smart grid: Optimised attack to gain momentary economic profit. *IET Gen. Transm. Distrib.* **2016**, *10*, 4032–4039. [CrossRef]
107. Sanjab, A.; Saad, W. Data Injection Attacks on Smart Grids with Multiple Adversaries: A Game-Theoretic Perspective. *IEEE Trans. Smart Grid* **2016**, *7*, 2038–2049. [CrossRef]
108. Khanna, K.; Panigrahi, B.K.; Joshi, A. AI-based approach to identify compromised meters in data integrity attacks on smart grid. *IET Gen. Transm. Distrib.* **2018**, *12*, 1052–1066. [CrossRef]
109. Wermann, A.G.; Bortolozzo, M.C.; da Silva, E.G.; Schaeffer-Filho, A.; Gaspary, L.P.; Barcellos, M. ASTORIA: A framework for attack simulation and evaluation in smart grids. In Proceedings of the NOMS 2016—2016 IEEE/IFIP Network Operations and Management Symposium, Istanbul, Turkey, 25–29 April 2016; pp. 273–280.
110. An, D.; Yang, Q.; Liu, W.; Zhang, Y. Defending Against Data Integrity Attacks in Smart Grid: A Deep Reinforcement Learning-Based Approach. *IEEE Access* **2019**, *7*, 110835–110845. [CrossRef]
111. Ren, L. Detecting Data Integrity Attacks on Correlated Solar Farms Using Multi-layer Data Driven Algorithm. In Proceedings of the 2018 IEEE Conference on Communications and Network Security, Beijing, China, 30 May–1 June 2018; pp. 1–9.
112. Ismail, M.; Shaaban, M.F.; Naidu, M.; Serpedin, E. Deep Learning Detection of Electricity Theft Cyber-Attacks in Renewable Distributed Generation. *IEEE Trans. Smart Grid* **2020**, *11*, 3428–3437. [CrossRef]
113. Yadav, S.A.; Kumar, S.R.; Sharma, S.; Singh, A. A review of possibilities and solutions of cyber-attacks in smart grids. In Proceedings of the 2016 1st International Conference on Innovation and Challenges in Cyber Security, ICICCS, Greater Noida, India, 3–5 February 2016; pp. 60–63.
114. Singh, V.K.; Ozen, A.; Govindarasu, M. Stealthy cyber attacks and impact analysis on wide-area protection of smart grid. In Proceedings of the NAPS 2016—48th North American Power Symposium, Denver, CO, USA, 18–20 September 2016.
115. Zhao, J.; Wang, J.; Yin, L. Detection and control against replay attacks in smart grid. In Proceedings of the 12th International Conference on Computational Intelligence and Security, CIS 2016, Wuxi, China, 16–19 December 2016; pp. 624–628.
116. Irita, T.; Namerikawa, T. Detection of replay attack on smart grid with code signal and bargaining game. In Proceedings of the American Control Conference, Seattle, WA, USA, 24–26 May 2017; pp. 2112–2117.

117. Velusamy, D. An Effective Trust Based Defense Mechanism to thwart Malicious Attack in Smart Grid Communication Network. In Proceedings of the 2017 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), Srivilliputtur, India, 23–25 March 2017.
118. Jiang, J.; Qian, Y. Defense Mechanisms against Data Injection Attacks in Smart Grid Networks. *IEEE Commun. Mag.* **2017**, *55*, 76–82. [CrossRef]
119. Xu, R.; Wang, R.; Guan, Z.; Wu, L.; Wu, J.; Du, X. Achieving Efficient Detection Against False Data Injection Attacks in Smart Grid. *IEEE Access* **2017**, *5*, 13787–13798. [CrossRef]
120. Patel, A. Destabilizing Smart Grid by Dynamic Load Altering Attack Using PI Controller. In Proceedings of the International Conference on Intelligent Computing, Instrumentation and Control Technologies, Kannur, Kerala, India, 6–7 July 2017; pp. 354–359.
121. Amini, S.; Mohsenian-Rad, H.; Pasqualetti, F. Dynamic load altering attacks in smart grid. In Proceedings of the 2015 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference, ISGT 2015, Washington, DC, USA, 18–20 February 2015; pp. 1–5.
122. Foroutan, S.A.; Salmasi, F.R. Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method. *IET Cyber-Phys. Syst. Theory Appl.* **2017**, *2*, 161–171. [CrossRef]
123. Fu, J.; Wang, L.; Hu, B.; Xie, K.; Chao, H.; Zhou, P. A Sequential Coordinated Attack Model for Cyber-Physical System Considering Cascading Failure and Load Redistribution. In Proceedings of the 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, China, 20–22 October 2018.
124. Zhou, X.; Li, Y.; Barreto, C.A.; Li, J.; Volgyesi, P.; Neema, H.; Koutsoukos, X. Evaluating Resilience of Grid Load Predictions under Stealthy Adversarial Attacks. In Proceedings of the 2019 Resilience Week (RWS), San Antonio, TX, USA, 4–7 November 2019; pp. 206–212.
125. Neema, H.; Volgyesi, P.; Koutsoukos, X.; Roth, T.; Nguyen, C. Online Testbed for Evaluating Vulnerability of Deep Learning Based Power Grid Load Forecasters. In Proceedings of the 8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, Sydney, Australia, 21 April 2020; pp. 1–6.
126. Nabil, M.; Ismail, M.; Mahmoud, M.M.E.A.; Alasmary, W.; Serpedin, E. PPETD: Privacy-Preserving Electricity Theft Detection Scheme with Load Monitoring and Billing for AMI Networks. *IEEE Access* **2019**, *7*, 96334–96348. [CrossRef]
127. Krundyshev, V.; Kalinin, M. Prevention of false data injections in smart infrastructures. In Proceedings of the 2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Sochi, Russia, 3–6 June 2019; pp. 1–5.
128. Ashrafuzzaman, M.; Chakhchoukh, Y.; Jillepalli, A.A.; Tosic, P.T.; de Leon, D.C.; Sheldon, F.T.; Johnson, B.K. Detecting Stealthy False Data Injection Attacks in Power Grids Using Deep Learning. In Proceedings of the 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, Cyprus, 25–29 June 2018; pp. 219–225.
129. Ayad, A.; Farag, H.E.Z.; Youssef, A.; El-Saadany, E.F. Detection of false data injection attacks in smart grids using Recurrent Neural Networks. In Proceedings of the 2018 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 19–22 February 2018.
130. Niu, X.; Li, J.; Sun, J.; Tomsovic, K. Dynamic Detection of False Data Injection Attack in Smart Grid using Deep Learning. In Proceedings of the 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 18–21 February 2019; pp. 1–6.
131. Trevizan, R.D.; Ruben, C.; Nagaraj, K.; Ibukun, L.L.; Starke, A.C.; Bretas, A.S.; McNair, J.; Zare, A. Data-driven Physics-based Solution for False Data Injection Diagnosis in Smart Grids. In Proceedings of the 2019 IEEE Power & Energy Society General Meeting (PESGM), Atlanta, GA, USA, 4–8 August 2019.
132. Esmalifalak, M.; Liu, L.; Nguyen, N.; Zheng, R.; Han, Z. Detecting Stealthy False Data Injection Using Machine Learning in Smart Grid. *IEEE Syst. J.* **2017**, *11*, 1644–1652. [CrossRef]
133. 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]
134. Wang, Z.; Chen, Y.; Liu, F.; Xia, Y.; Zhang, X. Power System Security Under False Data Injection Attacks With Exploitation and Exploration Based on Reinforcement Learning. *IEEE Access* **2018**, *6*, 48785–48796. [CrossRef]
135. Chen, Y.; Huang, S.; Liu, F.; Wang, Z.; Sun, X. Evaluation of Reinforcement Learning-Based False Data Injection Attack to Automatic Voltage Control. *IEEE Trans. Smart Grid* **2019**, *10*, 2158–2169. [CrossRef]
136. Pei, C.; Xiao, Y.; Liang, W.; Han, X. Detecting False Data Injection Attacks using Canonical Variate Analysis in Power Grid. *IEEE Trans. Netw. Sci. Eng.* **2020**. [CrossRef]
137. Esmalifalak, M.; Liu, L.; Nguyen, N.; Zheng, R.; Han, Z. Detecting stealthy false data injection using machine learning in smart grid. In Proceedings of the IEEE Global Communications Conference (GLOBECOM), Atlanta, GA, USA, 9–13 December 2013; pp. 808–813.
138. Albalushi, A.; Khan, R.; McLaughlin, K.; Sezer, S. Ontology-based approach for malicious behaviour detection in synchrophasor networks. In Proceedings of the IEEE Power & Energy Society General Meeting, Chicago, IL, USA, 16–20 July 2017; pp. 1–5.
139. Jillepalli, A.A.; de Leon, D.C.; Johnson, B.K.; Chakhchoukh, Y.; Oyewumi, I.A.; Ashrafuzzaman, M.; Sheldon, F.T.; Alves-Foss, J.; Haney, M.A. METICS: A Holistic Cyber Physical System Model for IEEE 14-bus Power System Security. In Proceedings of the 2018 13th International Conference on Malicious and Unwanted Software (MALWARE), Nantucket, MA, USA, 22–24 October 2018; pp. 95–102.

140. Hong, W.; Huang, D.; Chen, C.; Lee, J. Towards Accurate and Efficient Classification of Power System Contingencies and Cyber-Attacks Using Recurrent Neural Networks. *IEEE Access* **2020**, *8*, 123297–123309. [CrossRef]
141. Chakhchoukh, Y.; Liu, S.; Sugiyama, M.; Ishii, H. Statistical outlier detection for diagnosis of cyber attacks in power state estimation. In Proceedings of the 2016 IEEE Power and Energy Society General Meeting (PESGM), Boston, MA, USA, 17–21 July 2016; pp. 1–5.
142. Hink, R.C.B.; Beaver, J.M.; Buckner, M.A.; Morris, T.; Adhikari, U.; Pan, S. Machine learning for power system disturbance and cyber-attack discrimination. In Proceedings of the 7th International Symposium on Resilient Control Systems (ISRCS), Denver, CO, USA, 19–21 August 2014; pp. 1–8.
143. Wu, Y.; Mendis, G.J.; He, Y.; Wei, J.; Hodge, B. An Attack-Resilient Middleware Architecture for Grid Integration of Distributed Energy Resources. In Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, 15–18 December 2016; pp. 485–491.
144. Ali, S.; Li, Y. Learning Multilevel Auto-Encoders for DDoS Attack Detection in Smart Grid Network. *IEEE Access* **2019**, *7*, 108647–108659. [CrossRef]
145. Hasan, K.; Shetty, S.; Ullah, S. Artificial Intelligence Empowered Cyber Threat Detection and Protection for Power Utilities. In Proceedings of the 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC), Los Angeles, CA, USA, 12–14 December 2019; pp. 354–359.
146. Yan, J.; He, H.; Zhong, X.; Tang, Y. Q-Learning-Based Vulnerability Analysis of Smart Grid against Sequential Topology Attacks. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 200–210. [CrossRef]
147. Chen, L.; Yue, D.; Dou, C.; Chen, J.; Cheng, Z. Evaluation of cyber-physical power systems in cascading failure: Node vulnerability and systems connectivity. *IET Gen. Transm. Distrib.* **2020**, *14*, 1197–1206. [CrossRef]
148. Panthi, M. Anomaly Detection in Smart Grids using Machine Learning Techniques. In Proceedings of the 2020 First International Conference on Power, Control and Computing Technologies (ICPC2T), Raipur, India, 3–5 January 2020; pp. 220–222.
149. Valdes, A.; Macwan, R.; Backes, M. Anomaly Detection in Electrical Substation Circuits via Unsupervised Machine Learning. In Proceedings of the 2016 IEEE 17th International Conference on Information Reuse and Integration (IRI), Pittsburgh, PA, USA, 28–30 July 2016; pp. 500–505.
150. Elmrabit, N.; Zhou, F.; Li, F.; Zhou, H. Evaluation of Machine Learning Algorithms for Anomaly Detection. In Proceedings of the International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Dublin, Ireland, 15–19 June 2020; pp. 1–8.
151. Weisha, Z.; Jinguang, S.; Jiazhong, L. Machine Learning-Based System Electromagnetic Environment Anomaly Detection Method. In Proceedings of the 2018 International Conference on Smart Grid and Electrical Automation (ICSGEA), Changsha, China, 9–10 June 2018; pp. 115–117.
152. Botvinkin, P.V.; Kamaev, V.A.; Nefedova, I.S.; Finogeev, A.G.; Finogeev, E.A. Analysis, classification and detection methods of attacks via wireless sensor networks in SCADA systems. *Life Sci. J.* **2014**, *5*, 384–388.
153. Meir, K. Cyber-Attack Detection in SCADA Systems using Temporal Pattern. *Comput. Secur.* **2019**, *84*, 225–238.
154. Li, D.; Guo, H.; Zhou, J.; Zhou, L.; Wong, J.W. SCADAWall: A CPI-enabled firewall model for SCADA security. *Comput. Secur.* **2018**, *80*, 134–154. [CrossRef]
155. Leandros, A.M.; Jianmin, J.; Tiago, J.C. Combining ensemble methods and social network metrics for improving accuracy of OCSVM on intrusion detection in SCADA systems. *J. Inf. Secur. Appl.* **2016**, *30*, 15–26.
156. Tarek, C.; Latifa, H. A practical implementation of unconditional security for the IEC 60780-5-101 SCADA protocol. *Int. J. Crit. Infrastruct. Prot.* **2017**, 1–32. [CrossRef]
157. Van, H.N.; Quoc, T.T.; Yvon, B. SCADA as a service approach for interoperability of micro-grid. *Sustain. Energy Grids Netw.* **2016**, *8*, 26–36.
158. Massimo, F.; Michał Chora, R.K. Simulation Platform for Cyber-Security and Vulnerability Analysis of Critical Infrastructures. *J. Comput. Sci.* **2017**, *22*, 179–186.
159. Pramod, T.C.; Boroojeni, K.G.; Amini, M.H.; Sunitha, N.R.; Iyengar, S.S. Key pre-distribution scheme with join leave support for SCADA systems. *Int. J. Crit. Infrastruct. Prot.* **2018**, *24*, 111–125.
160. Kumar, N.R.; Mohanapriya, P.; Kalaiselvi, M. Development of an Attack-Resistant and Secure SCADA System using WSN, MANET, and Internet. *Int. J. Adv. Comput. Res.* **2014**, *4*, 627–633.
161. Lily, L.; Po, H. Vulnerability analysis of cascading dynamics in smart grids under load redistribution attacks. *Electr. Power Energy Syst.* **2019**, *111*, 182–190.
162. Shamsul, H.; John, Y.; Mohammed, M.H.; Ahmad, A. Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks. *Appl. Soft Comput.* **2018**, *71*, 66–77.
163. Shitharth, A.; Prince, W. An enhanced optimization-based algorithm for intrusion detection in SCADA network. *Comput. Secur.* **2017**, *70*, 16–26.
164. Yang, Z.; Han, R.; Wang, Y.; Gao, Y. Self-healing Control and Auto-measurement Technique for Smart Distribution Grid. In Proceedings of the 2019 International Conference on IC Design and Technology, Suzhou, China, 17–19 June 2019; pp. 1–5.

165. Sundararajan, A.; Wei, L.; Khan, T.; Sarwat, A.I.; Rodrigo, D. A Tri-Modular Framework to Minimize Smart Grid Cyber-Attack Cognitive Gap in Utility Control Centers. In Proceedings of the 2018 Resilience Week (RWS), Denver, CO, USA, 20–23 August 2018; pp. 117–123.
166. Roberts, C.; Scaglione, A.; Jamei, M.; Gentz, R.; Peisert, S.; Stewart, E.M.; McParland, C.; McEachern, A.; Arnold, D. Learning Behavior of Distribution System Discrete Control Devices for Cyber-Physical Security. *IEEE Trans. Smart Grid* **2020**, *11*, 749–761. [CrossRef]
167. Cai, W.; Yu, L.; Yang, D.; Zheng, Y. Research on Risk Assessment and Strategy Dynamic Attack and Defense Game Based on Twin Model of Power Distribution Network. In Proceedings of the 2017 IEEE 7th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), Honolulu, HI, USA,, 31 July–4 August 2017; pp. 684–689.
168. Chen, Y.; Gieseking, T.; Campbell, D.; Mooney, V.; Grijalva, S. A Hybrid Attack Model for Cyber-Physical Security Assessment in Electricity Grid. In Proceedings of the 2019 IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, 7–8 February 2019; pp. 1–6.
169. Li, J.; Liu, L.; Zhao, C.; Hamedani, K.; Atat, R.; Yi, Y. Enabling Sustainable Cyber Physical Security Systems through Neuromorphic Computing. *IEEE Trans. Sustain. Comput.* **2018**, *3*, 112–125. [CrossRef]
170. Cui, Y.; Bai, F.; Liu, Y.; Liu, Y. A Measurement Source Authentication Methodology for Power System Cyber Security Enhancement. *IEEE Trans. Smart Grid* **2018**, *9*, 3914–3916. [CrossRef]
171. Payne, E.K.; Wang, Q.; Shulin, L.; Wu, L. Technical risk synthesis and mitigation strategies of distributed energy resources integration with wireless sensor networks and internet of things—review. *J. Eng.* **2019**, *2019*, 4830–4835. [CrossRef]
172. Schumilin, A.; Stucky, K.; Sinn, F.; Hagenmeyer, V. Towards ontology-based network model management and data integration for smart grids. In Proceedings of the 2017 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), Pittsburgh, PA, USA, 18–21 April 2017; pp. 1–6.