energies

MDPI

Review

A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid

Shahid Tufail [1], Imtiaz Parvez [1], Shanzeh Batool [2] and Arif Sarwat [1,*]

[1] Department of Electrical and Computer Engineering, Florida International University, Miami, FL 33174, USA; stufa001@fiu.edu (S.T.); iparv001@fiu.edu (I.P.)
[2] School of Computer Science and Engineering, Vellore Institute of Technology, Sehore 466114, India; shanzeh.batool2019@vitbhopal.ac.in
* Correspondence: asarwat@fiu.edu

Abstract: The world is transitioning from the conventional grid to the smart grid at a rapid pace. Innovation always comes with some flaws; such is the case with a smart grid. One of the major challenges in the smart grid is to protect it from potential cyberattacks. There are millions of sensors continuously sending and receiving data packets over the network, so managing such a gigantic network is the biggest challenge. Any cyberattack can damage the key elements, confidentiality, integrity, and availability of the smart grid. The overall smart grid network is comprised of customers accessing the network, communication network of the smart devices and sensors, and the people managing the network (decision makers); all three of these levels are vulnerable to cyberattacks. In this survey, we explore various threats and vulnerabilities that can affect the key elements of cybersecurity in the smart grid network and then present the security measures to avert those threats and vulnerabilities at three different levels. In addition to that, we suggest techniques to minimize the chances of cyberattack at all three levels.

Keywords: smart grid; cyber attacks; DDoS attack; authentication; authorisation; packet flooding; denial of service

Citation: 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. https://doi.org/10.3390/en14185894

Academic Editor: Islam Safak Bayram

Received: 31 July 2021
Accepted: 11 September 2021
Published: 17 September 2021

1. Introduction

The conventional electricity system has been enhanced with modern technology, transforming it into a smart grid. A smart grid incorporates several operational and energy management techniques. The operational and energy measures may include smart meters and smart appliances installed at the customer's location, a production meter, renewable energy generators, smart inverters, and energy efficiency resources deployed at the grid's location [1]. Renewable energy generators contribute to energy cost reductions since the cost of producing electricity from renewable sources is zero, although renewable energy is intermittent in nature and is highly influenced by a variety of conditions such as ambient temperature, humidity, wind speed and direction, and geographical area. Solar energy, for example, is affected by irradiance, cloud cover, and ambient temperature [2]. Wind energy fluctuates greatly with wind speed and direction. Numerous techniques exist for forecasting wind energy, solar energy, and battery state of charge in order to incorporate renewable energy in a robust and timely way. The smart grid enables bidirectional communication between the grid and the sensors installed in various locations. These sensors continuously transmit production data to the grid in the form of data packets. This information covers the creation, consumption, voltage, and frequency of energy, as well as other energy-related data. Currently, battery-integrated grids send the state of charge over charge through a communication channel that exposes the battery management system (BMS) to cyber threats. These cyber threats can lead battery to overcharge or undercharge, which may lead to catastrophic events.

There are numerous benefits of the smart grid over traditional grids such as improved power quality, self-healing, cost effectiveness with the integration of renewable energy, adaptive energy generation, more environmentally friendly operation, aggregation of distributed energy resources (DERs), real-time energy consumption monitoring at customer's end, integration of AI models to automate tasks, remote energy motoring, rapid response to faults, remote fault location identification, and automated maintenance. These benefits make the smart grid more attractive than the traditional grid. The two main challenges that arise are cybersecurity and complexity. These issues become more challenging when the smart grid data is hosted on the cloud [3,4]. Apart from physical security, cybersecurity becomes a key element of the smart grid to keep it secure and stable all the time. Cyber protection is not only required for the smart grid but [5] shows even traditional and nonsmart grids are also exposed to cyberattacks. This study performed in [5] presents the impact on the grid when a malicious software(botnet) controls the overall power consumption including CPU, GPU, hard disks, screen brightness, and laser printers of computers. The simulation performed showed that 2.5 to 9.8 million infections can destabilize the grid. In another research [6], high wattage IoT devices can cause frequency instability, line failure, and increase in operating cost when the attacker the access to the IoT botnet of the high wattage smart appliances. These types of attacks have potential to cause major blackout by manipulating the energy demand.

As the complexity of the grid increases, the chances of faults also increase. For example, there are thousands of sensors installed and one of the sensors starts transmitting faulty data despite being no fault in the production devices; this can destabilize the whole functionality of the grid system. The second challenge is security—specifically, the communication between devices and the grid. The complexity of the communication channels of the smart may lead to problems in securing the smart grid data and cyberattack can lead to physical damage to the smart grid. The key contribution of this paper are (1) analysis of the communication network of the smart grid. The communication network is the backbone of smart grid, and it is the communication network that makes the grid a smart grid. (2) We performed an in-depth review of current vulnerabilities in the present smart grid and their mitigation techniques. (3) Any cyberattack targets either the communication network or employees working to manage the communication network or the customers using the network. We present techniques that can minimize the the chances of any cyberattack at any level.

The rest of the paper is organized as follows. In Section 2, we discuss the communication architecture of the smart grid followed by Section 3, which shows the various vulnerabilities in smart grid. In Section 4, the primary goals of cybersecurity in smart grid are discussed. In Section 5, we present a brief history of cyberattacks and blackouts around the world. In Section 6, we discuss the existing solutions to the cybersecurity problem of smart grid. In Section 7, open issues, challenges, and solutions are discussed, followed by the conclusion in Section 8.

2. Communication Architecture of Smart Grid

The components of the smart grid are depicted in Figure 1. A communication network connects the three domains: service provider, grid, and customer. This communication occurs across a variety of different protocols and channels. The grid domain encompasses large-scale energy generation, distribution, and transmission. The smart meter connects concurrently with the consumer domain and the communication network and this combined network is known as Advanced Metering Infrastructure(AMI) network. Smart meters are assigned to send data of consumption of use, outages, and electricity prices [7]. It communicates with the consumer domain using a short-range protocol such as Zigbee, and with the customer domain via GSM, Wi-Fi, and so on. While the smart grid enables more efficient energy distribution than the traditional centralized system, it is subject to security attacks at many tiers [8–13].

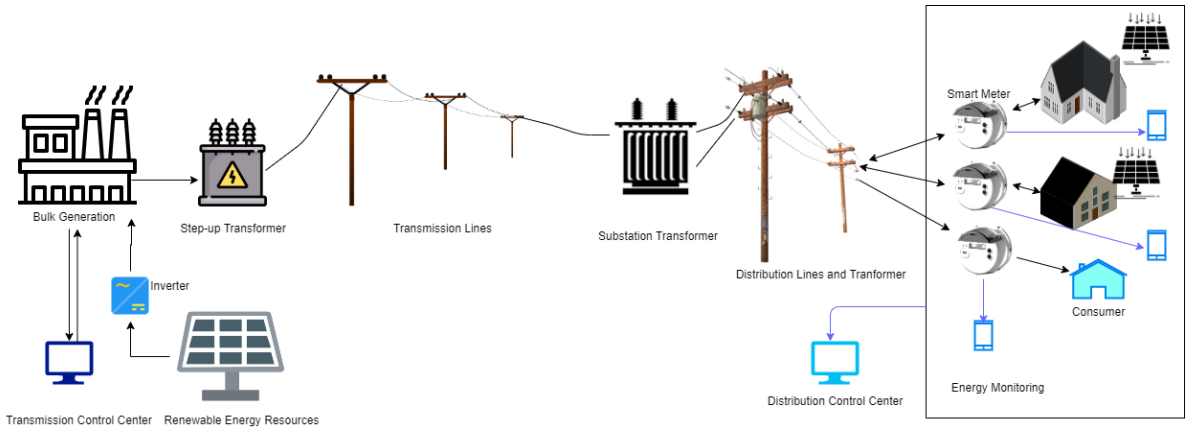

Figure 1. Smart grid architecture.

3. Vulnerabilities in the Smart Grid

The vulnerability of a smart grid network is the weak spot at which an attacker may enter the network and attack the system as shown in Figure 2. The smart grid connects with multiple domains using different protocols, making it vulnerable to numerous cyberattacks. In this section, we explore the conditions that might increase the vulnerability of the grid to cyber intrusion. However, first, we discuss the types of cyberattacks.There are mainly two kinds of attacks: (1) passive attacks and (2) active attacks. Passive attacks are those in which no harm to the data is done, but the attacker only monitors the data, whereas the active attacks are more dangerous compared to active attacks, as the attacker modifies the data or stops the receiver from receiving the data.

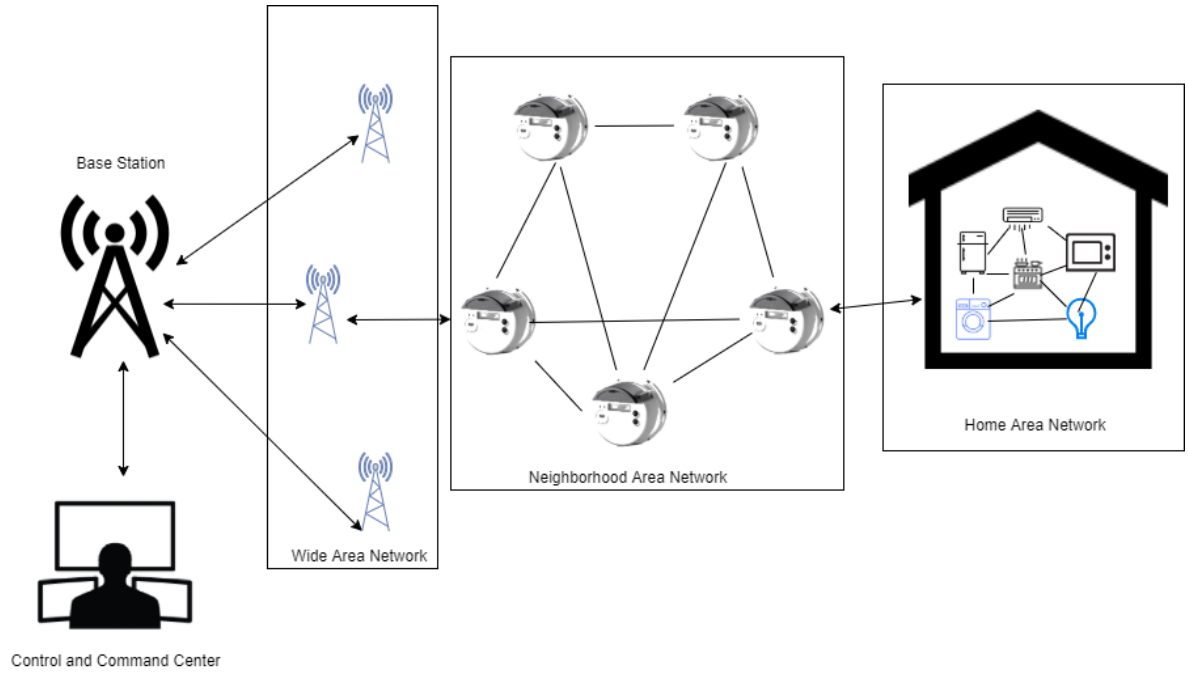

Figure 2. A segmentation of smart grid communication network.

The passive attacks are classified into two categories: (1) eavesdropping attack and (2) traffic analysis attacks. The types of active attacks includes masquerade attacks, replay attack, false data attack, and denial of service attacks.

Figure 3 shows different types of cyberattacks. The eavesdropping attacks is when the attacker can see the data packets shared between sender and the receiver. However, the attacker does not modifies the data. Traffic analysis attack is another kind of passive attack

in which the attacks continuously monitors and analyzes the traffic between the sender and the receiver. Active attacks are more harmful than the passive attacks, as the attacker has full control over the data. The replay attack is when the attacker and sender both send the data to the receiver; this confuses the receiver in differentiating between real data by sender and the data routed through the attacker. In the masquerade attack, the sender is idle, but the receiver keeps receiving data from the attacker. The false data injection attack in when the data do not come to the receiver directly from the sender instead the receiver receives the modified data from the attacker. However, both the sender and the receiver are unaware about the modification done by the attacker. Denial of service attack is a kind of attack in which attacker does not target the sender or receiver but the data server. The attacker generates a bulk amount of irrelevant requests from the server and the server starts serving those irrelevant requests until all of its resources are exhausted. The receiver/sender requests information from the server, and due to unavailability of resources, the request from the sender/receiver is denied. The major causes that make the smart grid vulnerable to cyberattacks are as follows:

1. Increased installation of intelligent electronic devices (IEDs): As the number of devices in the network rises, the number of attack sites for attackers increases as well. Even if the security of a single point is compromised, the entire network system would be impacted.
2. Installation of third-party components: Third-party components that are not advised by experts increase the network's vulnerability to cyberattack. These devices may be infected with trojans, which can then infect other devices on the network.
3. Inadequate personnel training: Proper training is necessary to operate any technology. When staff are not sufficiently taught, they might easily fall victim to phishing attempts.
4. Using Internet protocols: Not all protocols are secure when it comes to data transmission. Certain protocols transfer data in an unencrypted format. As a result, they are easy candidates for data extraction via man in the middle attacks.
5. Maintenance: While the primary goal of maintenance is to keep things functioning properly, it can become a vector for cyberattacks at times. While doing maintenance, operators often disable the security system to conduct testing. In 2015, electric power companies in eastern Europe reported one similar occurrence [14].

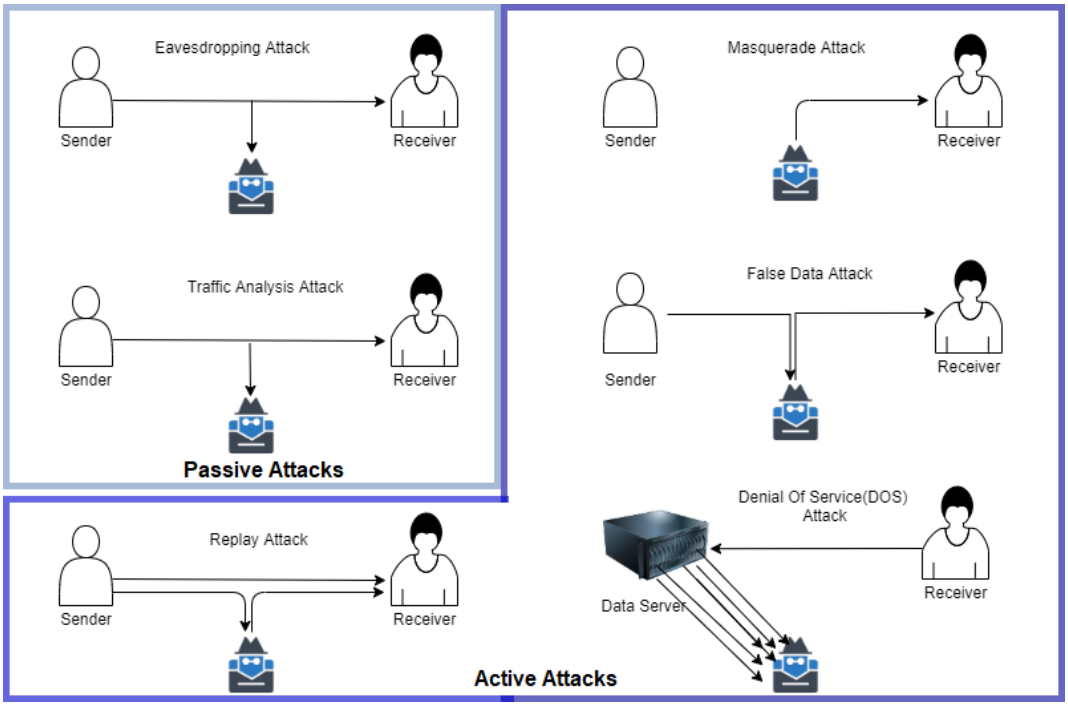

Figure 3. Types of cyber attacks.

Cybersecurity Challenges in Grid-Connected EV Charging Stations

The integration of electric vehicle charging system (EVCS) makes the power system/grid more complex. Over the past several years, the sales of electric vehicles have increased exponentially, mainly due to economic and environmental factors. With incorporation of newer technologies, the cost of EVs and EV batteries has seen a drastic decrease in addition to government incentives. Moreover, EVs do not rely on fossil fuel consumption so they are contributing in minimizing carbon footprints [15]. However, EVCSs are not cyberattack-resistant as they depend on the wired and wireless communication systems to share information with the smart grid. The study in [16] categorized EVCS vulnerabilities into two broad categories, i.e., internal vulnerability and external vulnerability. Internal vulnerability such as EVCS processor with weak password and hashing algorithm, weak access control, unsigned firmware update, and easy extraction of firmware can lead to attacker to get full control of EVCS. External vulnerabilities such as on-site human machine interface (HMI) that allow users to connect universal serial bus (USB) drives can be easily used by attackers to expose the EVCS configuration. Since there is no worldwide standard for communication systems between EVCSs and EVCS server, the open charge point protocol (OCPP) has been adopted by many vendors. However, OCPP is vulnerable to man-in-the-middle attack (MIMA) [16]. In addition to this, many smartphone and web-based applications that assist users in finding EVCSs nearby, authenticating EVs at EVCS, and remotely controlling the charging and payment for the charge have been developed. Due to this, any malicious application or cloned application can potentially damage the EVCS. In [17], the authors performed a study on cybersecurity challenges in the onboard charging (OBS) system of an EV. The electric component units (ECUs) are connected in a controller area network (CAN) to communicate between them. Cyberattacks on OBC system are classified into two categories: (1) control-based attacks and (2) hardware-based attacks. Figure 4 shows attacks included in both categories. The sales of EV are highly correlated with installation of EVCSs such that the EV penetration will go up, there will be a spike in EV charging stations, and there will be a significant impact on energy demand [18]. In this study, the communication requirement and standards for the Internet of electric vehicles are presented. In another research study, authors developed a framework for analysis, comparison, and test of standards (FACTS), proposed in [19], to identify cyberthreats in a battery management system (BMS).

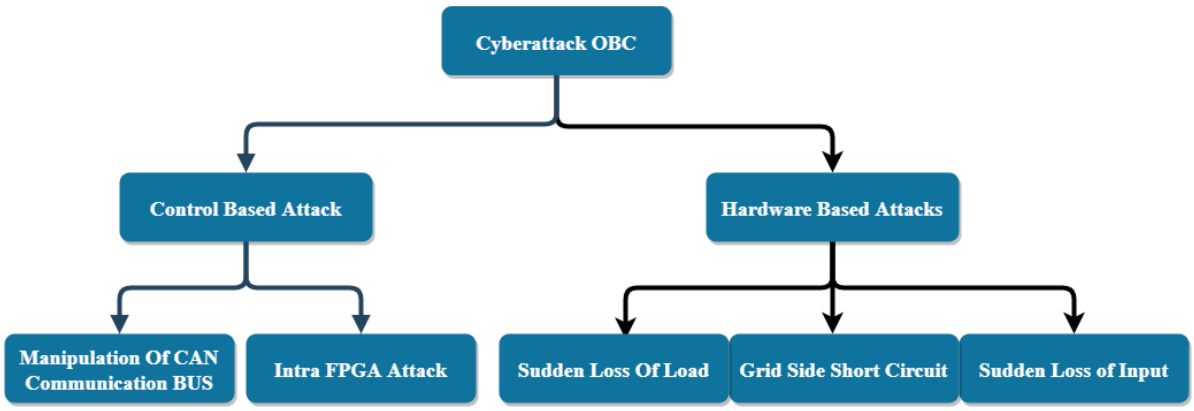

Figure 4. Cyberattack categories in OBC.

4. Primary Goals of the Cybersecurity in the Smart Grid

The National Institute of Standards and Technology (NIST) developed a framework for enhancing smart grid cybersecurity. They categorized logical interface categories in 22 different categories. Table 1 summarizes their definition along with example and their impact on confidentiality, integrity, and availability. Furthermore, the NIST suggests 19 smart grid requirements, which are as follows:

1. Awareness Training (SG.AT)

2. Access Control (SG.AC)
3. Audit and Accountability (SG.AU)
4. Security Assessment and Authorization (SG.CA)
5. Configuration Management (SG.CM)
6. Continuity of Operations (SG.CP)
7. Identification and Authentication (SG.IA)
8. Information and Document Management (SG.ID)
9. Incident Response (SG.IR)
10. Smart Grid Information System Development and Maintenance (SG.MA)
11. Media Protection (SG.MP)
12. Physical and Environmental Security (SG.PE)
13. Planning (SG.PL)
14. Security Program Management (SG.PM)
15. Personnel Security (SG.PS)
16. Risk Management and Assessment (SG.RA)
17. Smart Grid Information System and Services Acquisition (SG.SA)
18. Smart Grid Information System and Communication Protection (SG.SC)
19. Smart Grid Information System and Information Integrity (SG.SI)

Security requirement identifier, category, requirement, supplemental guidance, requirement enhancement, additional consideration, and impact level allocation should be added with each security requirement. Security requirement in depth can be presented in [20].

There are five main goals of cybersecurity in smart grids that are described below. Table 2 provides the summary of attack category and security goal they compromise.

1. *Authentication*: The verification of the user. The system verifies that the credentials provided by the user are correct or not. Various authentication techniques in the smart grid network are presented in the [21].
2. *Authorization*: The user is authenticated when he provides the correct credentials. Now, the user becomes authorized to use the services and to transmit and receive data packets. In an unencrypted authentication process, credential inserted by the users are exposed to the attacker, and later, the attacker uses the credentials and pretends to be an authorized user.
3. *Confidentiality*: This ensures that only authorized users have the access to the data. There is an abundance of sensitive data circulating throughout the smart grid network. This information comprises client energy consumption statistics, a customer identification number, and a list of appliances in use by consumers. An attacker can use this information to investigate the customer's energy use patterns. Additionally, if unauthorized users have access to the data, an ICMP (Internet Control Message Protocol) flood attack can be launched and the reading can be tampered with or altered [22]. As a result, utilities may face severe financial difficulties or customers may get excessively high bills.
4. *Integrity*: This protects the recipient against data tampering by ensuring that the data is not changed or corrupted during transmission. Parity check, checksum error, and several other similar techniques are utilized at the receiving end to verify that the data have not been modified. False data injection attack(FDIA) is one of the most frequently used forms of attack. An injection attack adulterates the genuine data with fake data.
5. *Availability*: Availability ensures that whenever user requires resources or/and data, they are always available. There are various factors that can affect the availability such as fault at the data center, but in terms of cybersecurity, it is affected by cyberattacks such as denial of service (DoS) attacks. During a DoS attack, the resources are hijacked by the attackers and user requests are not served due to a lack of resources.

Table 1. NIST Logical Interface Category Definition and Impact.

			Risks		
Logical Interface Category	**Definition**	**Example**	**Confidentiality**	**Integrity**	**Availability**
1	Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints,	Between transmission SCADA and substation equipment	Low	High	High
2	Interface between control systems and equipment without high availability but with compute and/or bandwidth constraints	Between distribution SCADA and lower priority pole-top equipment	Low	High	Medium
3	interface between control systems and equipment with high availability, without compute or bandwidth constraints,	Between transmission SCADA and substation automation systems	Low	High	High
4	Interface between control systems and equipment without high availability, without compute or bandwidth constraints,	Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs	Low	High	Medium
5	Interface between control systems within the same organization,	Multiple DMS systems belonging to the same utility	Low	High	High
6	Interface between control systems in different organizations	Between an RTO/ISO EMS and a utility energy management system	Low	High	Medium
7	Interface between back office systems under common management authority	Between a customer information system and a meter data management system	High	Medium	Low
8	Interface between back office systems not under common management authority,	Between a third-party billing system and a utility meter data management system	High	Medium	Low
9	Interface with B2B connections between systems usually involving financial or market transactions,	Between a retail aggregator and an energy clearinghouse	Low	Medium	Medium
10	Interface between control systems and noncontrol/corporate systems,	Between a work management system and a geographic information system	Low	High	Medium
11	Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements,	Between a temperature sensor on a transformer and its receiver	Low	Medium	Medium

Table 1. *Cont.*

			Risks		
Logical Interface Category	**Definition**	**Example**	**Confidentiality**	**Integrity**	**Availability**
12	interface between sensor networks and control systems	Between a sensor receiver and the substation master	Low	Medium	Medium
13	Interface between systems that use the AMI network,	Between MDMS and meters Between LMS/DRMS and Customer EMS	High	High	Low
14	Interface between systems that use the AMI network with high availability,	Between MDMS and meters Between LMS/DRMS and customer EMS Between DMS applications and customer DER	High	High	High
15	Interface between systems that use customer (residential, commercial, and industrial) site networks such as HANS and BANs	Between customer EMS and customer appliances Between customer EMS and customer DER	Low	Medium	Medium
16	Interface between external systems and the customer site	Between third-party and HAN gateway Between customer and CIS Web site	Low	Medium	Low
17	Interface between systems and mobile field crew laptops/equipment	Between field crews and GIS Between field crews and substation equipment	Low	High	Medium
18	Interface between metering equipment,	Between submeter to meter Between PEV meter and energy service provider	Low	High	Low
19	Interface between operations decision support systems	Between WAMS and ISO/RTO	Low	High	Medium
20	Interface between engineering/maintenance systems and control equipment	Between engineering and substation relaying equipment for relay settings	Low	High	Medium
21	Interface between control systems and their vendors for standard maintenance and service	Between SCADA system and its vendor	Low	High	Low
22	Interface between security/network/system management consoles and all networks and systems	Between a security console and network routers, firewalls, computer systems, and network nodes	High	High	High

Table 2. Security goals compromised under attack category.

Attack Category	Security Goal Compromised	Description	Reference
Flooding attack	Availability	Deterring users from utilizing the resources	[23,24]
Denial of service	Availability	Stop serving of users' request	[7,25–28]
Jamming	Availibility	Jamming the network	[29–31]
Buffer overflow	Availability, Confidentiality	Overwriting the memory of buffer	[32]
False Data Injection	Integrity	Tampering the real data	[33–36]
Social Engineering Attack	Integrity, Confidentiality	Attacking humans instead of machines or networks	[37–39]
Man-in-the-middle	Confidentiality	Extracting packet information between sender and receiver	[39–41]
Packet Sniffing	Confidentiality	Analyzing the packet	[42]
Session hijacking attack	Integrity, Confidentiality	Obstructing the user from resources for a particular amount of time	[43]
Data manipulation	Integrity	Data tampering	[44,45]
Replay Attack	Integrity	Send data, again and again.	[46–49]

5. Brief History of Cyberattacks on Smart Grids and Blackouts

5.1. Ukraine Power Grid Attack, 2015

Cyber assaults on the energy industry are on the rise, posing an ever-increasing threat to dependability and safety. This danger is shown by the successful assaults on Ukraine's power system in 2015 and 2016. During these incidents, attackers gained access to distribution grid operator consoles and remotely closed breakers, resulting in local blackouts. In this attack, 30 substations were switched off and around 230,000 people were affected by the blackout. It was the first successful known cyberattack on a smart grid. Attackers may potentially breach communications channels and alter data, or they could overwhelm the highly linked network with data traffic, restricting operators' capacity to monitor and manage the grid.

5.2. Iran Nuclear Facility Attack, 2010

Stuxnet is said to have caused many centrifuges at Iran's Natanz uranium enrichment plant to burn out. Stuxnet was designed to disrupt and sabotage Iran's nuclear program, but it also showed that Stuxnet had the potential to inflict significant physical damage to critical infrastructures by targeting computer controllers and SCADA systems that manage industrial equipment [50].

5.3. Blackout in US and Canada, 2003

On 14 August 2003, a high-voltage power line in northern Ohio collided with some overgrown trees, causing the fault. The line had weakened as a result of the strong current flowing through it. The issue would normally have triggered an alert in the control room, but the alarm system failed. Later, three more lines sagged into trees and shut down, putting further strain on other power lines. Due to overburden, they also cut off a couple of hours later, triggering a chain reaction of failures throughout southeastern Canada and eight northeastern states. In all, 50 million people lost power for up to two days in North America's largest blackout in history. At least 11 people were killed as a result of the incident, which is believed to have cost $6 billion. The details of the event can be found on [51].

5.4. Arizona–Southern California Blackout, 2011

A total of 2.7 million people were impacted by the 8 September 2011, Arizona–Southern California blackout. On a hot days demand during peak hours increases and due to this increase in demand, a single high-voltage line failed due to a fault, causing electricity to be transferred to the San Diego region. More line and transformer failures followed within minutes of this power redistribution, and ultimately, San Diego was cut off from the rest of Western Interconnection. A mismatch between supply and demand in the San Diego region arose from this separation, resulting in generation of overloads and blackouts [6].

6. Cyberattack Detection and Mitigation Techniques

Smart grids involves multiple stakeholders that includes consumers, electric utilities, grid operators, and third-party service providers. Due to involvement of multiple stakeholders, the management of the smart grid data specially from the smart meters becomes a daunting task. For enhanced security and privacy protection of smart meter, [52] proposed framework that provide guidelines for integrating security and privacy across different domain. The framework classifies the security into three classes: communication security, secure computing, and system control security. Communication security includes cryptosystem, routing security, and network privacy. The objectives of the communication security may be achieved by a key management system, end-to-end encryption, and multiple hop routing. Furthermore, the authors of [53] discussed primary tasks of smart meters that includes recording of amount of energy consumed and factors such as voltage and frequency. In addition, they are also responsible for sending the information to the grid operating over a secure communication channel and also to operate load switch during by operators to avoid blackouts during emergency cases. The study provided proof of concept of high assurance smart meters (HASM). To address the cybersecurity aspects of smart grid, various approaches have been suggested in the literature, and as the complexity and integration of artificial intelligence (AI) increases, more research studies on ways to make the grid more reliable will be conducted. Some research studies also show that the smart grid is also prone to human error, and those errors can be due to social engineering attacks. In our paper, we divided the existing approaches into two major categories: (1) nonhuman-centric approaces and (2) human-centric approaches. In Table 3, we summarize the advantages and disadvantages of both of the approaches.

6.1. Nonhuman-Centric Approaches

In this section, we discuss various nonhuman centric attack detection and mitigation techniques using the diverse approaches as summarized in Table 4.

6.1.1. Machine-Learning-Based Attack Detection and Mitigation

As the transition of traditional grid into smart grid is taking place, thousands of sensors are being installed in the smart grid infrastructure. These sensors continuously monitor the states of the device they are connected to and generate a huge amount of data in the form of log files or time series data. Irradiance sensor, module temperature sensor, voltage monitor sensor, and current monitor sensor are just a few examples of the sensors present in the smart grid network. The data from these sensors are stored on a server, and sometime before sending the data to the servers, these data are preprocessed. The servers can be local servers or cloud servers. Posting the data on the local server provides the highest level of data protection; however, it limits the strength of the data in finding new patterns or getting any insights from the data. When the data are stored on the cloud server, the user has more flexibility over data usage because the data can be access remotely and can be scrapped to machine using GETS command.

Recently, machine learning algorithms have proved to be accurate in cyberintrusion detection. Unlike rule-based methods, machine learning detects the intrusion based on historical data. In [54], a combination of JRipper and Adaboost was developed to predict

power system disturbances. The output of the model was three classes (attack, natural disturbances, and no event) based on the data. False data injection attack (FDIA)/data poisoning attack is another one of the most common attacks that carry the potential of severely damaging smart grid networks and FDIA can also harm utilities and customers financially by poisoning the data from smart meters. To detect an FDIA, researchers used an ensemble-based machine learning algorithm [55]. The model was tested on IEEE 14 bus system. The performance of ensemble-based learning models was compared with linear regression, naive Bayes, decision tree, and support vector machine (SVM), and the result shows that unsupervised ensemble models outperformed the individual models with the highest accuracy of 73%. In [56], deep analysis of the impact of FDIA on AI-based smart grid is performed using multilayer perceptron (MLP). The results from the study show that even if only 20% of the data is falsified, it can reduce the accuracy of the machine learning algorithms by 15% that can affect the critical decision making of the smart grid. For example, in the case of data poisoning, if there is disturbance and the model fails to predict the disturbance due to false data, then the grid can go into an unstable state that can result in catastrophic events. In [33], a conditional deep belief network model is proposed to detect FDIA for power theft in real time. The model was tested on IEEE 118 and IEEE 300 bus systems. The performance of the model was compared to artificial neural networks and support-vector-machine-based methods.

Sometimes, a smart grid also faces distributed denial of service (DDoS) attacks. DDoS attacks comprise the availability of the resources that are needed for communication such as servers. The primary objective of the DDoS attack is to inundate the communication server with fake requests to jam the server and make it unavailable for communication. In [57], a multilevel autoencoders model was proposed to detect DDoS attacks. Autoencoder consists of one input layer at least one hidden layer and one output layer. The model was trained using data of around 700 thousand packets and with 49 features. Source and destination IP and ports, source and destination jitters, record time, and attack category were some of their features. The UNSW-NB15 publicly available data set was used to develop the model. The results show that autoencoder-based prediction model performance was better than long short-term memory (LSTM), random forest, naïve Bayes, decision tree, *k*-nearest neighbor, and LSVM.

Table 3. Human-Centric vs. Nonhuman-Centric approaches.

Cyberattack Detection & Mitigation Techniques	Approach	Advantage	Disadvantages
Nonhuman-Centric	Machine-Learning-Based	1. High accuracy 2. Easy to deploy models 3.Task automation 4. Continous and adaptive learning	1. Highly data-oriented so as to get the best results historical data in bulk is need to train the model. 2. Training model takes a lot of time and is computationally expensive. 3. If hyperparameters are not tuned, then there are chances of overfitting or underfitting.
	Cloud-Computing-Based	1. Highly secure 2. Not computationally expensive 3. Low latency	1. High availability of bandwidth 2. Dependency on cloud service provider
	Blockchain-Based	1. Highly secure in general 2. Distributed data storage 3. Smart contract are immutable 4. All the transactions are encrypted	1. Few studies on blockchain-based cyber protection 2. High energy consumption to run all the nodes 3. Private blockchains are not secure.
Human-Centric	Multifactor authentication	Provides an addtional layer of security to the operator working in the command and control center	Not all employees are ready to embrace new technological changes as they find difficulty in adapting to new technology
	Employee Training	Employees in an organization can be categorized as attitudinal (employees who do not think that cybersecurity is an important factor to consider) and cognitive (employees who understand the importance but do not embrace it because they think its too much work) [58] therefore, regular employees training can be helpful in combatting cyberattacks.	Encouraging employees to teach themselves about the latest technologies and tools is a complex task, especially when the employees come from different age groups and with a variety of technical backgrounds.
	Password strength and security	Cognitive-type fatigue can lead to employees setting weak passwords [58]; thus, enforcing strong passwords and strength policy can be helpful.	As per [58], some employees find it difficult to remember all the of different and complex passwords.
	Customer Awareness	It is almost impossible to provide proper training to customers, so customer participation becomes critical to spread awareness about cybersecurity among customers.	Irrespective of how many resources an organization invests in customer awareness, at the end, customers are the key decision makers in the customer domain.
	Customer Interaction	A customer interaction platform can help with easy reporting of any cyberattack or any malicious activity on the customers' portal.	There is a huge variation in customer categories. For example, some customers are of different age groups, and some customers have a limited sense of technology, so it becomes challenging to design a portal that fits all.
	Updates and incremental patches installation	Patching policy varies between immediate, 30, 60, and 90 days [59] depending upon the potential impact of the vulnerability or bug; therefore, patching can be highly impactful in tackling future cyberattacks.	No Even systems armored with the best security tools and software are always under threat; thus, continous monitoring and auditing are required for robust protection.

6.1.2. Cloud-Based Detection and Mitigation

In [60], the authors discussed how the attributes of cloud computing could be used to enhance security in the event of a DDoS attack on the smart grid. In [61], a cloud-based firewall was proposed to prevent DDoS attacks on the smart grid. The study was performed by generating 250 Gbps of data to replicate a DDoS attack. The simulation results showed that there was low latency with the grid OpenFlow firewall. In [62], an attribute-based online/offline searchable encryption scheme was introduced in order to secure data access for authorized users in the cloud environment for smart grid applications. In [63], the authors introduced a secure home area network based on cloud of things, which is detrimental against brute force, replay and capture, and other attacks. In [64], a security evaluation model was proposed for a smart grid based on a deep belief network (DBN) comprised of multiple RBMs and a BP neural network. They evaluated security risks in five respects: policy and organizational risks, general technical risks, SaaS risks, PaaS risks, and IaaS risks.

6.1.3. Blockchain-Based Detection and Mitigation

In recent times, blockchain has become one of the most lucrative technologies in various domains due to its security. The blockchain is a chain of blocks in which each block contains the index, timestamp, previous hash, hash, and data. Blockchain is considered to be secure because of the hashing. If someone tries to change the hash value of the block, then he has to change the value of all the previous blocks, so when there are many blocks in the chain, it becomes a computationally expensive task to change the hashes of all of the previous blocks.

In [65], the authors proposed a policy architecture based on blockchain for the exchange of data between independent system operations and underoperating agents to protect against FDIA. The model contains three layers: (1) the data layer, (2) the detection layer, and (3) the blockchain layer. The data layer is responsible for the collection of data, the collected data are transferred to the detection layer for community detection, and the blockchain layer keeps the community detection and transaction record secure. In their research, the authors of [66] proposed a blockchain-based secure message transfer method for smart meters and service providers. The method prevents FDIA on the smart meter side. In this study, each transaction is initiated by the smart meters and the service provider is the master node. The transaction information is shared over the network and periodically validated by auditing and broadcasting of transactions. Service providers are connected in a peer-to-peer (P2P) network fashion. To add a new transaction/block, consensus verification is needed, and only after verification is the new block added. A key is generated using the SHA-256 algorithm at every transaction. Using the blockchain-based structure, the authors showed in this study that data can be exchanged within a P2P service provider network. In the study [67], a decentralized security model based on the lightning network and smart contract in the blockchain ecosystem was introduced. This model includes registration, scheduling, authentication, and charging phases. The authors of [68] proposed a novel framework with a combination of integrated hardware security and blockchain scheme for the grid-edge devices to maintain a distributed cybersecurity technique that verifies the provenance of messages both from and to the devices.

6.1.4. Hardware-Based Security

IoT devices are one of the most critical parts of the smart grid network. Theses devices are responsible for data collection and analysis and sending the data over the communication channel, and also at the same time, they need to be armored to combat any cyberattack [69]. Some of the key hardware security problems were discussed in [70]. These security problems includes physical attacks, side channel analysis, and hardware Trojans. In the physical attack, the attacker tries to bypass the authentication system. During the physical attack, the attacker exploits the vulnerabilities in the implemented system that they find using reverse engineering. In side channel analysis, the attacker uses the profile

of the features such as current, voltage, and frequency to predict the cryptographic keys. A hardware Trojan is any change or addition made to a circuit with the intent of causing harm. Unauthorized access of private information, manipulation of circuit functioning, and reduction of circuit reliability are some of the primary objectives of hardware Trojans. The authors of [71] proposed methods to detect hardware trojan using path delay fingerprint.

Smart meters, sensors, and communication devices, among other IoT devices, face a number of difficult challenges, including low energy usage and a shortage of computing capabilities [72]. Physical unclonable functions (PUFs) offer completely secure authentication without the device containing any cryptographic capabilities, as it requires more computational resources; thus PUFs are particularly appealing for resource-limited IoT devices. However, with the evolution of machine learning, which is highly capable of predicting behavior using historical data/events, PUFs' behavior can also be predicted with 95% accuracy [73]. To protect PUFs against machine-learning-based attacks, the authors of [73] proposed a configurable tristate PUF (CTPUF), which used an XOR-based mechanism to ambiguate the relationship between the challenge and response. This ambiguity makes the machine learning model unable to draw any pattern between the challenge and response. The results in this study showed the accuracy of machine learning, including support vector machine (SVM), artificial neural network (ANN), and logistic regression model after CTPUF was about 60%. Another research showed the limitations of voltage-overscaling (VOS)-based authentication, as it can be exploited using machine learning models (ML) [74]. In this study, an ML-resistant VOS method that integrated previous challenges with keys was proposed. The results showed that the accuracy of the ML model after challenge self-obfuscation structure (CSoS) was about 51.2%.

Table 4. Types of attacks and their detection and prevention techniques.

Attack Category	Detection/Mitigation Technique Type	Proposed Solution/Research performed	Target of Attack	Reference
Flooding attack	Time measurement of flooded packets	Bait-Message-Based Detection	Communication network	[23,24]
Denial of service (DoS)	——	Impact of DoS in AMI network	AMI Network	[7]
DoS	——	Impact of DoS on load frequency control	Load frequency controller	[26]
FDIA	Deep Machine Learning	Conditional Deep Belief Network (CDBN)	SCADA network	[33]
FDIA	Machine Learning	Ensemble-Based Learning	AMI Network	[55]
Social Engineering Attack (SEA)	——	Impact of SEA on industrial control system security by measuring the mean time to compromise under attack	Humans at organizations	[38]
FDIA	Machine Learning	Multilayer Neural Network to study the impact of FDIA in Artificial-Intelligence-Based Smart Grid	Communication Network	[33]
FDIA	Machine Learning	Artificial neural network model to predict presence of cyber attack	Communication network to poison PV generation data	[36]
SEA	——	Studied 37 intrusion detection and prevention system and proposed appropriate IDPS	SCADA and AMI	[37]
FDIA	Blockchain	Blockchain-based secure message transfer method for smart meters and service providers	Smart Meters	[66]

Table 4. *Cont.*

Attack Category	Detection/Mitigation Technique Type	Proposed Solution/Research performed	Target of Attack	Reference
DDoS	Cloud computing	Computing capability of cloud	Communication network	[60]
DDoS	Cloud computing	Cloud-based firewall	Communication network	[61]
Data manipulation	Cloud computing	Attribute-based online/offline searchable encryption scheme	AMI and SCADA	[63]
Social Engineering, Data Manipulation, and Session Hijacking	Cloud computing	Deep Belief Network	SCADA	[64]

6.2. Human-Centric Mitigation Approaches

In this section, we discuss various human-centric attack detection and mitigation approaches.

6.2.1. Employee Protection at Command and Control Center Technique

1. Multifactor Authentication (MFA): As referred to Figure 5, this protects data from unauthorized access to data. The complexity of the password-breaking program increases exponentially when two sequential authentication processes are integrated. This minimizes the chance of unauthorized users getting access to the data.
   SMS token authentication, email token authentication, hardware token authentication, software token authentication, and phone authentication are some of the techniques that are currently used for multifactor authentication in various domains. When the user clears the first pass, he is redirected to one of the authentication methods in the second pass. All of the passwords/pin generated in the second pass are valid for single login. In an SMS token system, the user receives a unique pin number that can be between 4 to 8 digits over his phone. Similar to an SMS token, in an email token, the user receives the pin over his verified email address. There are various algorithms used to generate the random code after each login. The generation procedure is out of the scope of this paper. The hardware token is one of the most secured multifactor authentications and mainly used in sectors in which data security is highly critical such as banking, insurance, or healthcare. In this, the user needs to insert the hardware token into their device to use it. Software token MFA is little bit similar to the SMS token, and in this authentication system, instead of getting the one-time password through wireless service provider, the user receives it in an application. The software token provides a level of security almost similar to that of a hardware token, but in software token MFA, the user's device is treated as hardware. The phone MFA can be through SMS, such as an SMS token, or a user can receive a call to verify his identity.
2. Employee training: Advancements in technology have made attacks on smart appliances more difficult such that hackers are target humans. Machine learning approaches are playing a key role for attackers in recognizing employees' behaviors and reactions in different situations. Not all humans have the same level of knowledge about technology, and they adapt to the environment at their own pace if no training is provided. This makes humans easy targets for attackers. According to [33], social engineering attacks are the second most common attacks after malware. Ransomware is one of the most recent attack methods through which humans are targeted instead of directly targeting the machine. Employee training is one of the key requirements for cyberattack aversion. In the smart grid network, the end users at command and control centers are human beings. Proper training helps them to avoid any social engineering attacks such as phishing and ransomware. Any successful phishing

attack gives complete control of the grid to the attackers and consequences can be catastrophic.

Another common type of attack that can be minimized by employee training is an insider attack. An insider attack occurs when any disgruntled employee uses the resources/access given to him to harm the organization. Employee training can beneficial to avert these attacks, as in that case, the employee will know what action he should take if he is not happy with the organization. Employee training can help to train workers to report any unusual behavior in their colleagues.

3. Password Strength: Strong passwords reduces the chances of integrity and confidentiality attack. Weak passwords are more vulnerable to password-guessing attacks. Password guessing is the mechanism by which the attacker tries to obtain entry to a system by guessing passwords (and often usernames) to get the target device login. Additionally, to perform the attack, the attacker uses the network resources and bandwidth which limits the resources for legitimate users. These attacks are performed remotely and generate a large volume of log data. The password strength is specified in terms of information entropy, which is measured in bits. For instance, if a password is 32 bits, then by a brute force method, an attacker will need to make 2^{32} attempts to crack the password—the stronger the password, the harder it is to crack. Strong passwords can make it almost impossible to guess the password, which is one of the viable methods to stop the intruder.

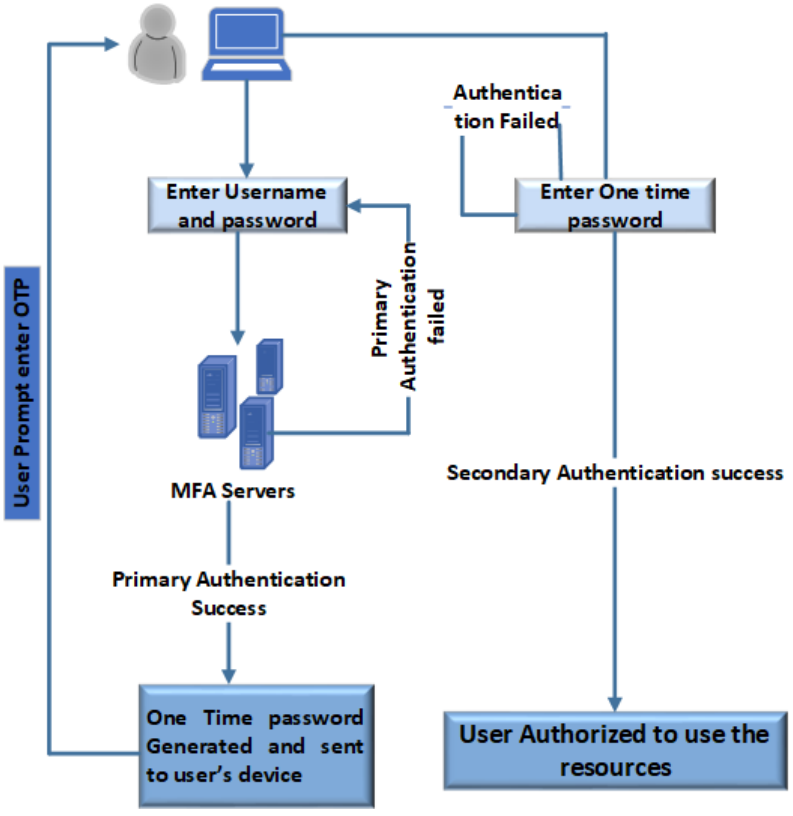

Figure 5. Working of multifactor authentication.

6.2.2. Customer Protection Technique

1. Operating system protection: Customers are one of the weakest links in the cybersecurity chain, and a major challenge with customers is that they cannot be systematically trained like employees. Thus, devices themselves, such as smart meters and smart inverters, need to be protected. The most efficient way to bar customers from customizing the internal operating system of the device is to make them tamper-proof. Another reason for a secured operating system is to stop customers from manipulat-

ing the reading of the meter. According to [75], a rigged smart meter can cost utility providers a huge loss, as the customers will be underpaying their bills.

2. Notifying customers: Recommending the best possible methods to customers is another approach to protection based on their current setting. For example, if a customer is using the utility application on his handheld device and the operating system on his device is outdated, this can make him an easy target of an attacker to exploit the vulnerabilities. Every customer is important. Even if an attacker is successful in breaching one customer's privacy, he can grab enough information to increase his chances for a successful next attack.
3. Software and hardware security: Apart from protecting the device against attack through the network, customers should protect their devices physically by having strong entry-level passwords for their devices. Customers providing minute and personal details to their friends can make them victims of password-guessing attacks. Sharing the password with friends can lead to an attacker installing bots to monitor the device and even taking full control of the device [76].
4. Protection against third-party applications: Customers should always be cautious about an application asking for permissions. Customers store sensitive information on their device, and some third-party applications ask for more information than they actually need. Around 98.5% of customers either pay no attention or sometimes pay attention to the permissions required by the applications, and 93.6% of users accept the terms and conditions of the application either instantly or within 1 min [77].
5. Cyberattack reporting: Utilities should build a platform where the customers can easily report any suspected attack. As the difference between the time of attack and and the time of report increases, the damage caused exponentially grows. A delay in reporting of attack puts not only one customer's privacy at risk but the privacy of other customers at stake as well. The most viable solution for this is to have a 24*7 customer support that can guide customers to the necessary actions to be taken at the time of attack.

7. Open Issues, Challenges, and Future Research Directions

As smart grids are environmentally friendly, they employ many of these renewable energy sources, and above all, they are safer than traditional power grids, they are better than traditional power grids in terms of efficiency and productivity [78]. The findings also revealed that the smart grid may also be vulnerable to cyberattacks. The advantages of using a smart grid in general will improve the security of cyberattack problems using a wide range of technologies and techniques. However, when conducting the study, multiple sources demonstrated the safety advantages and vulnerability associated with intelligent grids. Almost all research studies show that a denial-of-service attack would be a major issue for smart grids. Because intelligent grids are constructing the network, a network attack will render the smart grid inoperable. The smart grid would maintain service availability while providing several layers of security, utilizing the virtual private network (VPN) to increase secure communication, IPS, and IDS as the best security features. Smart grid and traditional grid are always at risk of human error. These errors may be due to overburdened employees, as it restricts their decision making capability, or it may be due to social engineering or insider attacks if employees are not trained to handle such kind of attacks. Attacks such as ransomware have increased by 500% since 2018, and that needs immediate attention, as ransomware attacks lead to huge losses and leaks of confidential information. Although some researchers have studied the impact of ransomware [79,80], more research is required to analyze the impact and reasons behind ransomware attacks in smart grid infrastructure.

Additionally, it is critical to be self-aware of cyberattacks on smart grids [78]. To protect the smart grid from various cyberattacks, the user should educate themselves on and mitigate the risks associated with the smart grid by doing various risk analysis and case studies. Furthermore, the study addressed possible difficulties associated with the smart

grid. The issue with intelligent grids is that they connect disparate devices over huge networks of geographical locations. Therefore, the primary issue becomes protecting this equipment from the larger infrastructure. By enabling the sharing and encryption of data, blockchain technology may be beneficial for addressing security concerns posed by malicious nodes or hackers [81]. Additionally, it may be used to authenticate identities and give access to transactions by storing and documenting them in an integrated database, as well as enabling smooth and cost-effective data transfers across scattered devices. Computer network protocols must be updated to reflect the present state of communication and to incorporate modern encryption technologies and security countermeasures, according to [82]. As a result, protection against emerging cyber threats is given.

Numerous difficulties occur from numerous attacks on the security of smart grid systems, as the smart grid's safety requirements and objectives are dispersed across large areas [83]. Due to the critical importance of power infrastructure and the socioeconomic impact of blackouts, the smart grid may be a primary target of cyber terrorism [83,84]. Cyber defense solutions should be used to safeguard all components of smart grid systems. Defensive solutions should incorporate a variety of defense technologies, including machine learning [85], proactive IDS/IPS systems, wireless controlled propagation, authorization, authentication, and certification [83,84]. The solutions should incorporate scalable, resilient, and adaptive cybersecurity/defense approaches for intelligent grid operations that do not jeopardize genuine smart grid operations.

8. Conclusions

Risks are inherent in innovation, and the move from a conventional to a smart grid adds another layer of complexity. In addition to maintaining and developing a strong physical architecture for the smart grid, it is exceedingly challenging to build, operate, and maintain the communication network architecture. This study performed a deep analysis on the smart grid communication network and did an in-depth review of the potential cyberattacks and their mitigation techniques.

No attack is insignificant; even the tiniest strike might result in disastrous consequences. A solution was presented to build a robust smart grid network by securing customers, the smart grid's communication network, and its employees, as we believe not only that the communication network is vulnerable to cyberattacks, but also that the people who use or manage it are equally vulnerable and can become an easy target of the attacker if they do not properly handle the attacks.

Author Contributions: Conceptualization, S.T. and I.P.; Funding acquisition, A.S.; Methodology, S.T.; Investigation, S.T.; Resources, I.P.; Supervision, I.P. and A.S.; Writing-original draft preparation, S.T.; Writing-review & editing, I.P. and S.B. All authors have read and agreed to the published version of the manuscript.

Funding: These materials are a result of research supported by the National ScienceFoundation under the award number CMMI-1745829 and CNS-1553494.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The study did not report any data.

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

References

1. FERC. *Federal Energy Regulatory Commission Assessment of Demand Response & Advanced Metering*; Federal Energy Regulatory Commission: Washington DC, USA, 2020. Available online: https://www.ferc.gov/industries-data/electric/power-sales-and-markets/demand-response/reports-demand-response-and (accessed on 30 March 2021).
2. Benger, S.N.; Zhou, S.; Guan, H. A dynamic solar irradiance model for assessing solar PV power generation potential in urban areas. In Proceedings of the 2014 International Conference and Utility Exhibition on Green Energy for Sustainable Development (ICUE), Jomtien Beach, Thailand, 19–21 March 2014; pp. 1–4.

3. Tufail, S.; Qadeer, M.A. Cloud Computing in Bioinformatics: Solution to Big Data Challenge. *Int. J. Comput. Sci. Eng.* **2017**, *5*, 232–236. [CrossRef]
4. Parvez, I.; Ahmed, A.; Dharmasena, S.; Tufail, S.; Sundararajan, A. Latency Critical Data Processing in Cloud for Smart Grid Applications. In *Advances in Information and Communication*; Arai, K., Ed.; Springer International Publishing: Cham, Switzerland, 2021; pp. 663–676.
5. Dabrowski, A.; Ullrich, J.; Weippl, E.R. Grid Shock: Coordinated Load-Changing Attacks on Power Grids: The Non-Smart Power Grid is Vulnerable to Cyber Attacks as Well. In Proceedings of the 33rd Annual Computer Security Applications Conference, Orlando, FL, USA, 4–8 December 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 303–314,
6. Soltan, S.; Mittal, P.; Poor, H.V. BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid. In Proceedings of the 27th USENIX Security Symposium (USENIX Security 18), Baltimore, MD, USA, 15–17 August 2018; USENIX Association: Baltimore, MD, USA, 2018; pp. 15–32.
7. 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, NSW, Australia, 10–14 June 2014; pp. 1029–1034.
8. Bari, A.; Jiang, J.; Saad, W.; Arunita, J. Challenges in the Smart Grid Applications: An Overview. *Int. J. Distrib. Sens. Netw.* **2014**, *2014*, 1–11. [CrossRef]
9. Ericsson, G.N. Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure. *IEEE Trans. Power Deliv.* **2010**, *25*, 1501–1507. [CrossRef]
10. Knapp, E.D.; Samani, R. Chapter 4—Privacy Concerns with the Smart Grid. In *Applied Cyber Security and the Smart Grid*; Knapp, E.D., Samani, R., Eds.; Syngress: Boston, MA, USA, 2013; pp. 87–99.
11. McLaughlin, S.; Podkuiko, D.; McDaniel, P. Energy Theft in the Advanced Metering Infrastructure. In *Critical Information Infrastructures Security*; Rome, E., Bloomfield, R., Eds.; Springer: Berlin/Heidelberg, Germany, 2010; pp. 176–187.
12. Asghar, M.R.; Dan, G.; Miorandi, D.; Chlamtac, I. Smart Meter Data Privacy: A Survey. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2820–2835.
13. Cleveland, F.M. Cyber security issues for Advanced Metering Infrasttructure (AMI). In Proceedings of the 2008 IEEE Power and Energy Society General Meeting—Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, USA, 20–24 July 2008; pp. 1–5.
14. Gauci, A.; Michelin, S.; Salles, M. Addressing the challenge of cyber security maintenance through patch management. *CIRED-Open Access Proc. J.* **2017**, *2017*, 2599–2601. [CrossRef]
15. Kumar, R.R.; Alok, K. Adoption of electric vehicle: A literature review and prospects for sustainability. *J. Clean. Prod.* **2020**, *253*, 119911. [CrossRef]
16. Acharya, S.; Dvorkin, Y.; Pandžić, H.; Karri, R. Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective. *IEEE Access* **2020**, *8*, 214434–214453. [CrossRef]
17. Chandwani, A.; Dey, S.; Mallik, A. Cybersecurity of Onboard Charging Systems for Electric Vehicles—Review, Challenges and Countermeasures. *IEEE Access* **2020**, *8*, 226982–226998. [CrossRef]
18. Bayram, I.S.; Papapanagiotou, I. A survey on communication technologies and requirements for internet of electric vehicles. *EURASIP J. Wirel. Commun. Netw.* **2014**, *2014*, 223. [CrossRef]
19. Khalid, A.; Sundararajan, A.; Hernandez, A.; Sarwat, A. FACTS Approach to Address Cybersecurity Issues in Electric Vehicle Battery Systems. In Proceedings of the 2019 IEEE Technology & Engineering Management Conference (TEMSCON), Atlanta, GA, USA, 12–14 June 2019.
20. Pillitteri, V.; Brewer, T. *Guidelines for Smart Grid Cybersecurity, 2014-09-25*; NIST Interagency/Internal Report (NISTIR); National Institute of Standards and Technology: Gaithersburg, MD, USA, 2014. [CrossRef]
21. Agarkar, A.; Agrawal, H. A review and vision on authentication and privacy preservation schemes in smart grid network. *Secur. Priv.* **2019**, *2*, e62, [CrossRef]
22. Shuaib, K.; Trabelsi, Z.; Abed-Hafez, M.; Gaouda, A.; Alahmad, M. Resiliency of Smart Power Meters to Common Security Attacks. *Procedia Comput. Sci.* **2015**, *52*, 145–152. [CrossRef]
23. Zhang, F.; Mahler, M.; Li, Q. Flooding attacks against secure time-critical communications in the power grid. In Proceedings of the 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), Dresden, Germany, 23–27 October 2017; pp. 449–454. [CrossRef]
24. Lu, Z.; Lu, X.; Wang, W.; Wang, C. Review and evaluation of security threats on the communication networks in the smart grid. In Proceedings of the 2010—MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE, San Jose, CA, USA, 31 October–3 November 2010; pp. 1830–1835.
25. Huseinovic, A.; Mrdovic, S.; Bicakci, K.; Uludag, S. A Taxonomy of the Emerging Denial-of-Service Attacks in the Smart Grid and Countermeasures. In Proceedings of the 2018 26th Telecommunications Forum (TELFOR), Belgrade, Serbia, 20–21 November 2018; pp. 1–4.
26. Liu, S.; Liu, X.P.; El Saddik, A. Denial-of-Service (dos) attacks on load frequency control in smart grids. In Proceedings of the 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 24–27 February 2013; pp. 1–6.
27. Huseinović, A.; Mrdović, S.; Bicakci, K.; Uludag, S. A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid. *IEEE Access* **2020**, *8*, 177447–177470. [CrossRef]

28. Cameron, C.; Patsios, C.; Taylor, P.C.; Pourmirza, Z. Using Self-Organizing Architectures to Mitigate the Impacts of Denial-of-Service Attacks on Voltage Control Schemes. *IEEE Trans. Smart Grid* **2019**, *10*, 3010–3019. [CrossRef]
29. Kurt, M.N.; Yilmaz, Y.; Wang, X. Real-Time Detection of Hybrid and Stealthy Cyber-Attacks in Smart Grid. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 498–513. [CrossRef]
30. Chatfield, B.; Haddad, R.J.; Chen, L. Low-Computational Complexity Intrusion Detection System for Jamming Attacks in Smart Grids. In Proceedings of the 2018 International Conference on Computing, Networking and Communications (ICNC), Maui, HI, USA, 5–8 March 2018; pp. 367–371.
31. Gai, K.; Qiu, M.; Ming, Z.; Zhao, H.; Qiu, L. Spoofing-Jamming Attack Strategy Using Optimal Power Distributions in Wireless Smart Grid Networks. *IEEE Trans. Smart Grid* **2017**, *8*, 2431–2439. [CrossRef]
32. Ying, H.; Zhang, Y.; Han, L.; Cheng, Y.; Li, J.; Ji, X.; Xu, W. Detecting Buffer-Overflow Vulnerabilities in Smart Grid Devices via Automatic Static Analysis. In Proceedings of the 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chengdu, China, 15–17 March 2019; pp. 813–817. [CrossRef]
33. He, Y.; Mendis, G.J.; Wei, J. Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism. *IEEE Trans. Smart Grid* **2017**, *8*, 2505–2516. [CrossRef]
34. Cui, L.; Qu, Y.; Gao, L.; Xie, G.; Yu, S. Detecting false data attacks using machine learning techniques in smart grid: A survey. *J. Netw. Comput. Appl.* **2020**, *170*, 102808. [CrossRef]
35. Deng, R.; Liang, H. False Data Injection Attacks With Limited Susceptance Information and New Countermeasures in Smart Grid. *IEEE Trans. Ind. Inform.* **2019**, *15*, 1619–1628. [CrossRef]
36. Riggs, H.; Tufail, S.; Khan, M.; Parvez, I.; Sarwat, A.I. Detection of False Data Injection of PV Production. In Proceedings of the 2021 IEEE Green Technologies Conference (GreenTech), Denver, CO, USA, 7–9 April 2021; pp. 7–12,
37. Singh, V.K.; Ebrahem, H.; Govindarasu, M. Security Evaluation of Two Intrusion Detection Systems in Smart Grid SCADA Environment. In Proceedings of the 2018 North American Power Symposium (NAPS), Fargo, ND, USA, 9–11 September 2018; pp. 1–6,
38. Green, B.; Prince, D.; Busby, J.; Hutchison, D. The Impact of Social Engineering on Industrial Control System Security. In Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, CPS-SPC '15, Denver, CO, USA, 16 October 2015; Association for Computing Machinery: New York, NY, USA, 2015; pp. 23–29.
39. 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]
40. Pour, M.M.; Anzalchi, A.; Sarwat, A. A review on cyber security issues and mitigation methods in smart grid systems. In Proceedings of the SoutheastCon 2017, Concord, NC, USA, 30 March–2 April 2017; pp. 1–4.
41. Rajendran, G.; Sathyabalu, H.V.; Sachi, M.; Devarajan, V. Cyber Security in Smart Grid: Challenges and Solutions. In Proceedings of the 2019 2nd International Conference on Power and Embedded Drive Control (ICPEDC), Chennai, India, 21–23 August 2019; pp. 546–551.
42. Shitharth, S.; Winston, D.P. A novel IDS technique to detect DDoS and sniffers in smart grid. In Proceedings of the 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), Coimbatore, India, 29 February–1 March 2016; pp. 1–6.
43. Pandey, R.K.; Misra, M. Cyber security threats—Smart grid infrastructure. In Proceedings of the 2016 National Power Systems Conference (NPSC), Bhubaneswar, India, 19–21 December 2016; pp. 1–6.
44. Wang, X.; Shi, D.; Wang, J.; Yu, Z.; Wang, Z. Online Identification and Data Recovery for PMU Data Manipulation Attack. *IEEE Trans. Smart Grid* **2019**, *10*, 5889–5898. [CrossRef]
45. Wang, J.; Shi, D.; Li, Y.; Chen, J.; Ding, H.; Duan, X. Distributed Framework for Detecting PMU Data Manipulation Attacks With Deep Autoencoders. *IEEE Trans. Smart Grid* **2019**, *10*, 4401–4410. [CrossRef]
46. 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; pp. 2112–2117.
47. Zhao, J.; Wang, J.; Yin, L. Detection and Control against Replay Attacks in Smart Grid. In Proceedings of the 2016 12th International Conference on Computational Intelligence and Security (CIS), Wuxi, China, 16–19 December 2016; pp. 624–627.
48. Cebe, M.; Akkaya, K. A Replay Attack-Resistant 0-RTT Key Management Scheme for Low-Bandwidth Smart Grid Communications. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6.
49. Alohali, B.; Kifayat, K.; Shi, Q.; Hurst, W. Replay Attack Impact on Advanced Metering Infrastructure (AMI). In *Smart Grid Inspired Future Technologies*; Hu, J., Leung, V.C.M., Yang, K., Zhang, Y., Gao, J., Yang, S., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 52–59.
50. Kenney, M. Cyber-Terrorism in a Post-Stuxnet World. *Orbis* **2015**, *59*, 111–128. [CrossRef]
51. *Blackout 2003: Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*; Technical Report; Department Of Energy: Washington, DC, USA, 2004. Available online: https://www.energy.gov/sites/default/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf (accessed on 27 August 2021).
52. Kalogridis, G.; Sooriyabandara, M.; Fan, Z.; Mustafa, M.A. Toward Unified Security and Privacy Protection for Smart Meter Networks. *IEEE Syst. J.* **2014**, *8*, 641–654. [CrossRef]

53. Mühlberg, J.T.; Cleemput, S.; Mustafa, M.A.; Van Bulck, J.; Preneel, B.; Piessens, F. An Implementation of a High Assurance Smart Meter Using Protected Module Architectures. In *Information Security Theory and Practice*; Foresti, S., Lopez, J., Eds.; Springer International Publishing: Cham, Switzerland, 2016; pp. 53–69.
54. Borges Hink, R.C.; 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 2014 7th International Symposium on Resilient Control Systems (ISRCS), Denver, CO, USA, 19–21 August 2014; pp. 1–8.
55. 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]
56. Tufail, S.; Batool, S.; Sarwat, A.I. False Data Injection Impact Analysis In AI-Based Smart Grid. In Proceedings of the SoutheastCon 2021, Atlanta, GA, USA, 10–13 March 2021; pp. 1–7. [CrossRef]
57. Ali, S.; Li, Y. Learning Multilevel Auto-Encoders for DDoS Attack Detection in Smart Grid Network. *IEEE Access* **2019**, *7*, 108647–108659. [CrossRef]
58. Reeves, A.; Delfabbro, P.; Calic, D. Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *SAGE Open* **2021**, *11*. [CrossRef]
59. Mugarza, I.; Flores, J.L.; Montero, J.L. Security issues and software updates management in the industrial internet of things (iiot) era. *Sensors* **2020**, *20*, 7160. [CrossRef]
60. Califano, A.; Dincelli, E.; Goel, S. Using features of cloud computing to defend smart grid against DDoS attacks. In Proceedings of the 10th Annual Symposium on Information Assurance (Asia 15), Albany, NY, USA, 2–3 June 2015; pp. 44–50.
61. Diovu, R.C.; Agee, J.T. A cloud-based openflow firewall for mitigation against DDoS attacks in smart grid AMI networks. In Proceedings of the 2017 IEEE PES PowerAfrica, Accra, Ghana, 27–30 June 2017; pp. 28–33. [CrossRef]
62. Eltayieb, N.; Elhabob, R.; Hassan, A.; Li, F. An efficient attribute-based online/offline searchable encryption and its application in cloud-based reliable smart grid. *J. Syst. Archit.* **2019**, *98*, 165–172. [CrossRef]
63. Alohali, B.; Merabti, M.; Kifayat, K. A cloud of things (cot) based security for home area network (han) in the smart grid. In Proceedings of the 2014 IEEE Eighth International Conference on Next Generation Mobile Apps, Services and Technologies, Oxford, UK, 10–12 September 2014; pp. 326–330.
64. Chen, L.; Liu, J.; Ha, W. Cloud service security evaluation of smart grid using deep belief network. *Int. J. Sens. Netw.* **2020**, *33*, 109–121. [CrossRef]
65. 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* **2021**, *13*, 90. [CrossRef]
66. Zhang, H.; Wang, J.; Ding, Y. Blockchain-based decentralized and secure keyless signature scheme for smart grid. *Energy* **2019**, *180*, 955–967. [CrossRef]
67. Huang, X.; Xu, C.; Wang, P.; Liu, H. LNSC: A Security Model for Electric Vehicle and Charging Pile Management Based on Blockchain Ecosystem. *IEEE Access* **2018**, *6*, 13565–13574. [CrossRef]
68. Saha, S.S.; Gorog, C.; Moser, A.; Scaglione, A.; Johnson, N.G. Integrating Hardware Security into a Blockchain-Based Transactive Energy Platform. In Proceedings of the 2020 52nd North American Power Symposium (NAPS), Tempe , AZ, USA, 11–14 April 2021; pp. 1–6.
69. Ghasempour, A. Internet of Things in Smart Grid: Architecture, Applications, Services, Key Technologies, and Challenges. *Inventions* **2019**, *4*, 22. [CrossRef]
70. Qu, G. Hardware Security and Trust: A New Battlefield of Information. In Proceedings of the Decision and Game Theory for Security—11th International Conference, GameSec 2020, College Park, MD, USA, 28–30 October 2020; Zhu, Q., Baras, J.S., Poovendran, R., Chen, J., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2020; Volume 12513, pp. 486–501. [CrossRef]
71. Jin, Y.; Makris, Y. Hardware Trojan detection using path delay fingerprint. In Proceedings of the 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, Anaheim, CA, USA, 9 June 2008; pp. 51–57.
72. Babaei, A.; Schiele, G. Physical Unclonable Functions in the Internet of Things: State of the Art and Open Challenges. *Sensors* **2019**, *19*, 3208. [CrossRef]
73. Zhang, J.; Shen, C.; Guo, Z.; Wu, Q.; Chang, W. CT PUF: Configurable Tristate PUF against Machine Learning Attacks for IoT Security. *IEEE Internet Things J.* **2021**,
74. Zhang, J.; Shen, C.; Su, H.; Arafin, M.T.; Qu, G. Voltage Over-scaling-based Lightweight Authentication for IoT Security. *IEEE Trans. Comput.* **2021**,
75. Hock, D.; Kappes, M.; Ghita, B. Using multiple data sources to detect manipulated electricity meter by an entropy-inspired metric. *Sustain. Energy Grids Netw.* **2020**, *21*, 100290. [CrossRef]
76. Jang-Jaccard, J.; Nepal, S. A survey of emerging threats in cybersecurity. *J. Comput. Syst. Sci.* **2014**, *80*, 973–993. Special Issue on Dependable and Secure Computing. [CrossRef]
77. May, Z.E.; Kaffel Ben Ayed, H.; Machfar, D. State of the art on Privacy Risk Estimation Related to Android Applications. In Proceedings of the 2019 15th International Wireless Communications Mobile Computing Conference (IWCMC), Tangier, Morocco, 24–28 June 2019; pp. 889–894.

78. Faquir, D.; Chouliaras, N.; Sofia, V.; Olga, K.; Maglaras, L. Cybersecurity in smart grids, challenges and solutions. *AIMS Electron. Electr. Eng.* **2021**, *5*, 24–37.
79. Zimba, A.; Chishimba, M. On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems. *Eur. J. Secur. Res.* **2019**, *4*, 3–31. [CrossRef]
80. Paquet-Clouston, M.; Haslhofer, B.; Dupont, B. Ransomware Payments in the Bitcoin Ecosystem. *arXiv* **2019**, arXiv:1804.04080.
81. Kimani, K.; Oduol, V.; Langat, K. Cyber security challenges for IoT-based smart grid networks. *Int. J. Crit. Infrastruct. Prot.* **2019**, *25*, 36–49. [CrossRef]
82. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2020**, *169*, 107094. [CrossRef]
83. Rawat, D.B.; Bajracharya, C. Cyber security for smart grid systems: Status, challenges and perspectives. In Proceedings of the IEEE SoutheastCon 2015, Fort Lauderdale, FL, USA, 9–12 April 2015; pp. 1–6.
84. The Essential Role of Cyber Security in the Smart Grid. Available online: https://electricenergyonline.com/energy/magazine/312/article/The-Essential-Role-of-Cyber-Security-in-the-Smart-Grid-.htm (accessed on 30 July 2021).
85. Ferrag, M.A.; Maglaras, L.; Moschoyiannis, S.; Janicke, H. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *J. Inf. Secur. Appl.* **2020**, *50*, 102419. [CrossRef]