energies

MDPI

Review

Review of Cybersecurity Analysis in Smart Distribution Systems and Future Directions for Using Unsupervised Learning Methods for Cyber Detection

Smitha Joyce Pinto [1,*], Pierluigi Siano [2,3,*] and Mimmo Parente [3]

[1] Department of Electronics and Communication, MIT Mysore, Belawadi, Srirangapatna 571438, India
[2] Department of Electrical and Electronic Engineering Science, University of Johannesburg, Johannesburg 2092, South Africa
[3] Dipartimento di Scienze Aziendali—Management & Innovation Systems, Università degli Studi di Salerno, 84084 Fisciano, Italy
* Correspondence: smithapinto_ece@mitmysore.in or smitha_joyce@yahoo.co.in (S.J.P.); psiano@unisa.it (P.S.)

Abstract: In a physical microgrid system, equipment failures, manual misbehavior of equipment, and power quality can be affected by intentional cyberattacks, made more dangerous by the widespread use of established communication networks via sensors. This paper comprehensively reviews smart grid challenges on cyber-physical and cyber security systems, standard protocols, communication, and sensor technology. Existing supervised learning-based Machine Learning (ML) methods for identifying cyberattacks in smart grids mostly rely on instances of both normal and attack events for training. Additionally, for supervised learning to be effective, the training dataset must contain representative examples of various attack situations having different patterns, which is challenging. Therefore, we reviewed a novel Data Mining (DM) approach based on unsupervised rules for identifying False Data Injection Cyber Attacks (FDIA) in smart grids using Phasor Measurement Unit (PMU) data. The unsupervised algorithm is excellent for discovering unidentified assault events since it only uses examples of typical events to train the detection models. The datasets used in our study, which looked at some well-known unsupervised detection methods, helped us assess the performances of different methods. The performance comparison with popular unsupervised algorithms is better at finding attack events if compared with supervised and Deep Learning (DL) algorithms.

Keywords: Association Rule Mining; clustering; cyber-attacks; data mining; FDIA; smart grid

check for updates

Citation: Pinto, S.J.; Siano, P.; Parente, M. Review of Cybersecurity Analysis in Smart Distribution Systems and Future Directions for Using Unsupervised Learning Methods for Cyber Detection. *Energies* **2023**, *16*, 1651. https://doi.org/10.3390/en16041651

Academic Editor: Wencong Su

Received: 19 December 2022
Revised: 2 February 2023
Accepted: 4 February 2023
Published: 7 February 2023

Copyright: © 2023 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 growing integration of Distribution Energy Resources (DER) into the electric grid, including photovoltaics (PV), wind, battery storage, fuel cells, and hydro schemes, has benefits, in that it lowers the cost of enhancing the power system, as well as drawbacks, particularly environmental uncertainty. For efficient and continuous operation, a microgrid controller that coordinates and regulates the various DER using communication technologies based on established communication protocols is essential [1]. Concerns with feeders, grid failure, communication, cyber security, control, islanding, regulation issues, and protection are some of the specific difficulties associated with the development of DER consumption into the grid [2]. However, because communication networks are so widely used, they are sensitive to harmful cyber-attacks. These attacks can be particularly dangerous if they result in physical harm to devices, technical failures, or human error. Physical and cyber security implies frequently threats that target power utilities [3]. Microgrid systems are more susceptible to cyberattacks because they are more dependent on distributed, active network control as their number of components grows, which raises the potential impact of an intrusion. According to a western US department of energy report from May 2019, the utility's wind and solar power generation installations were

disconnected, its supervisory control and data acquisition (SCADA) systems experienced a brief outage, and the network was temporarily disconnected for five minutes [4,5]. Both physical harm and financial loss can result from a cyberattack that introduces instability or incorrect information into the electrical system. Microgrid operators and developers require a comprehensive and integrated approach to cyber-physical safety to be more adaptable. Strengthening the microgrid, a systematic review of the interconnection security controls, designing and formulation of disaster management, and reserves for the security procedure are the essentials to guarantee the safety of the key energy configuration [6].

Many kinds of cyber-attacks can jeopardize the data and communication security of the smart grids, including False Data Injection Attacks (FDIAs) [7], Distributed Denial of Service (DDoS) attacks [8], topological attacks [9], overloading attacks [10], and resonance attack [11]. FDIAs have excellent accessibility, interference, and concealment capabilities, making them one of the most dangerous attack tactics in many power cyber-attacks [12]. FDIA may cause either the automated system or the operator to take incorrect action. As a result, it leads to incorrect decision-making and control procedures, which ultimately has fatal effects. In this kind of attack, hackers might use physical, cybernetic, and cyber-physical channels to fraudulently obtain important information. FDIA seeks to alter data at the measuring units or control center to achieve a certain goal. The nodal voltage magnitudes and angles, nodal power injections, line power flows, and digital data such as the state of breakers and switches are among the analog measured data from the power system that FDIAs aim to capture. To monitor and manage the operation of the power grid through analysis of meter measurement data, the power system operator (PSO) needs to execute state estimation (SE). At the transmission system level, the issue of detecting cyberattacks through flawed data processing in state estimators has recently attracted a lot of attention [13].

The SE method's central concept is the estimation of each area's state using measurements specific to that area and the sharing of boundary bus states between adjacent areas. In energy management systems, SE algorithms play a crucial role in the processing of inaccurate measurements. When bad data are present, it is anticipated that large residual errors will inevitably result from the bad data, hence bad data detection (BDD) filters measurement inaccuracies brought on by malicious assaults or device flaws. However, when a successful FDIA is started, the residual error would remain the same as usual. To safeguard state estimates, certain strategies for faulty measurement detection have been developed [14].

Analyzing the power system model is not necessary for the contemporary BDD methodologies based on data-driven models. To anticipate measurement error, they apply the ML approach to extract the electrical attributes from the massive historical data. The next step is to utilize clustering analysis to automatically group good and bad data into distinct clusters [15]. For selecting the most important features to detect FDIA and remove bad data, we reviewed unsupervised machine learning methods on smart grids.

This paper gives a comprehensive review of the field of cyber-attacks against smart grids and introduces the background of state estimation. This paper examines cyber-attack detection through unsupervised data mining algorithms. Clustering and Association Rule Mining (ARM) are two different categories under unsupervised techniques. With various advantages over supervised and reinforcement algorithms, ARM and clustering are data mining techniques used to calculate the correlation between two or more variables in a dataset by identifying the strongest rules that exist between their values. On another side, the unsupervised approach of clustering has a low detection rate with tampered data. As a result, this article offers a thorough assessment of numerous unsupervised methodologies and approaches tailored to the difficulties posed by cyberattacks on smart grids, as well as an analysis of their characteristics.

The structure of this article is as follows: In Section 2 the review methodology is described and in Section 3 we will provide a general review of the cyber security issues with smart grid technologies. Section 4 explains FDIA approaches and techniques in smart

grids. Section 5 discusses the unsupervised learning-based detection techniques for cyber-attacks over FDIA. Sections 6 and 7 outline future studies and conclusions, respectively.

2. Review Methodology

The main goal of this review is to provide a platform for researchers to summarize various cyber-attack detection techniques on smart grids and explain the best one of those attacks. This review offers a thorough explanation of numerous attacks, highlights their benefits and drawbacks, discusses present trends and suggested directions for the future, and offers a thorough evaluation of the various publications. Significant academic publications were searched for electronically in databases such as IEEE Explore, Springer, Wiley, PubMed, Science Direct, Frontiers, MDPI, Research Gate, and Google Scholar. The publications were gathered using a variety of criteria, including keywords, journals, conferences, different attacks, ML or DL approaches, classifier performance, and feature extraction techniques. All accessible research publications published between 2015 and 2022 that used Data Mining (DM) applications for diagnosing or forecasting cyberattacks on smart grids met the screening criteria for this study. The following characteristics were coded for each article: (a) main research area within dialect studies; (b) geographical location of the cyber-attack on smart grids (e.g., Israel-2016, France-2018, US-2019, Portugal-2020); (c) security requirements (e.g., integrity, confidentiality, availability); (d) key points of ML features (e.g., supervised, unsupervised, semi-supervised, reinforcement); (e) classification type; (f) system parameters (e.g., support, lift, confidence); (g) year of publication; (h) communication networks (e.g., LAN, MAN, BAN, NAN, HAN); (i) I/O sensors (e.g., RTU, PDC, PMU); (j) evaluation criteria; (k) communication layers (e.g., application, transport, MAC, network, physical); (l) attack category (e.g., SCADA, smart meter, physical, data injection, and replay, networks based); and (m) attacking cycle (e.g., reconnaissance, scanning, maintenance access, exploitation). The number of articles reviewed by year of publication and cyber-attack-affected smart grids is shown in Figure 1.

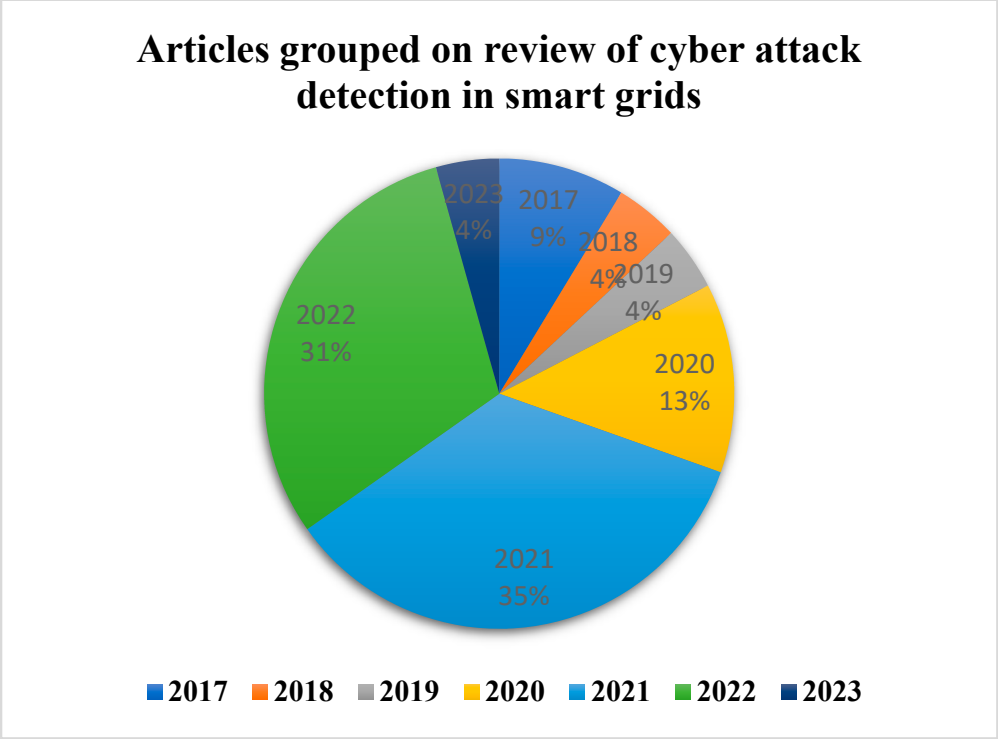

Figure 1. Year-wise publications with the search of cyber-attack reviews in various publications.

Table 1 provides a comparison between the existing survey papers in terms of the main covered areas and publication year. Few reviews [16–21] are more focused on the

sensor and communication-related topics during cyber-attacks. Some other reviews [22,23] covered all topics of cyber-attack such as the nature of attacks, characteristics of the attack, monitoring in smart grid, existing co-simulation tools, testbed, and awareness. Other works focused on cyber-attack detection and mitigation techniques [19,24]. We have concluded that the twenty-two reviews were more focused on the ML approach considered to be the best method for the detection and mitigation of cyber-attacks in smart grids. In these review papers, unsupervised learning algorithms have not received much interest. Therefore, we considered unsupervised type ML for identifying FDIA cyber-attack in smart grids which differs from the aforementioned surveys. Clustering and association rules are two unsupervised algorithm analyses that can help locate hidden patterns and potential relationships between variables that commonly appear together in datasets. This method can be used to evaluate network traffic, identify patterns of cyberattacks in smart grids, and analyze and anticipate user behavior.

Table 1. Comparison between existing journal's review work.

Ref No./Year	Sensor Technologies	Communication Technologies	Computing Technologies	Type of Cyber Attack	Detection	Contributions	Limitations
[25]/2020	No	No	Yes	FDIA	No	Studied FDIA against SE and degrade the microgrids inducing a power imbalance between supply and demand	Detection and mitigation techniques
[16]/2018	yes	yes	No	Virus, DOS, replay, Man in middle attacks	Yes Limited approach	Comprehensive overview of cyber-security in the smart grid and examined the main cyber-attacks threatening its structure, network protocols, and applications.	Machine learning techniques
[26]/2021	No	No	No	Attacks on CIA model.	No	Analyses the threats and potential solutions of smart grids based on IoT.	Detection techniques
[27]/2021	No	No	No	FDIA	No	Discussed two modeling frameworks for CPSs, FDIAs against state estimation, vulnerabilities, and dynamical properties of attacks	Sensor, communication, and detection techniques
[17]/2023	yes	yes	No	No	No	Overview of SG model, key elements, ADMS, SCADA, AMI, cyber security principles, standards, and protocols.	Detection techniques
[22]/2022	No	No	No	Physics aware control command, measurement integrity, FDI, control logic modification, DOS, etc.	yes	A complete review of the nature of complex cyber-attacks, detection and monitoring capabilities, Cyber-Physical Situational Awareness, IDS-based host, network, cloud, IoT, signature, distributed, anomaly, ML/DL, hybrid, moving target defense, specification, etc.	Sensor, communication technologies.
[24]/2022	No	No	yes	Described several types of cyber attack	yes	A broad analysis of the system structure and vulnerabilities of typical inverter-based power systems with DER integration, several types of cyberattacks, modern defense strategies including several detection and mitigation techniques, and comparison of testbed and simulation tools applicable for cyber-physical research.	Communication protocols and networks, sensor measurement
[28]/2022	yes	yes	No	yes	yes	Discussed approaches to ML, AI, 5G, blockchain, and data aggregation methods.	Limited approach to sensor technologies
[29]/2021	No	No	No	FDIA	yes	Cyber-attack enhancement methods, challenges, and resilience of the smart grid.	Sensor, communication technologies.

Table 1. *Cont.*

Ref No./Year	Sensor Technologies	Communication Technologies	Computing Technologies	Type of Cyber Attack	Detection	Contributions	Limitations
[23]/2022	No	No	No	yes	yes	Presented attack strategy, detection methods, and solutions for cyberattacks in terms of blockchain technology and AI techniques.	Sensor and communication technologies.
[18]/2021	yes	yes	No	FDIA, DOS	yes	Various threats and vulnerabilities can affect the key elements of cyber security in the smart grid network and then present the security measures.	Limited approach to ML and blockchain techniques.
[19]/2021	yes	yes	yes	All types of attacks mentioned	yes	Inclusive review of the cyber-physical attacks, vulnerabilities, mitigation approaches on the power electronics, and the security challenges for the smart grid applications.	The limited approach in ML detection techniques
[30]/2020	No	No	No	All types of attacks mentioned	yes	Summarizes impacts of cyber-attacks on power system control, power system stability, and types of cyber-attacks, from the viewpoints of topology, mechanism, probability, and simulation.	Communication sensors, and limited approach to detection techniques
[31]/2021	yes	yes	yes	Aurora, pricing, AGC, FDI, topology, GPI-spoofing, load redistribution, line outage masking, Stuxnet-like networks	No	Reviewed an abstracted and combined state-space model, in which cyber-physical attack and defense models are effectively widespread, and advanced in the field, moving target defense, watermarking, and data-driven approaches.	Detection techniques
[32]/2012	yes	No	No	No	No	Significance of cyber infrastructure security in conjunction with power application security to prevent, mitigate, and tolerate cyber-attacks.	Cyber-attacks, communication, and detection techniques.
[33]/2017	No	No	No	FDIA	No	A comprehensive review of the theoretical and mathematical approach of FDIAs against modern power systems.	Detection strategy of FDIA
[20]/2021	yes	yes	yes	No	IDS	Discussed in detail rule learning-based intrusion detection systems.	Limited approach to detection techniques.
[34]/2017	No	No	No	yes	No	Introduced CPS, distinguishing between cyber, cyber-physical, and physical components security perspective, a taxonomy of threats, susceptibilities, attacks, and controls.	Detection techniques
[35]/2019	yes	yes	Yes	All types of attacks mentioned	Limited approaches and types mentioned	The approach of ML in security concerns. Overview of big data tools, system platforms, required skill levels, CIA models, encryption algorithms, software attacks, and their countermeasures	ML detection techniques
[21]/2021	yes	yes	yes	No	No	This survey is focused on IOT technologies that facilitate smart energy grid systems, architecture, related software standard applications, security vulnerabilities, and opportunities to integrate advanced techniques.	Cyber-attacks and detection systems

Table 1. *Cont.*

Ref No./Year	Sensor Technologies	Communication Technologies	Computing Technologies	Type of Cyber Attack	Detection	Contributions	Limitations
[36]/2022	No	No	yes	DOS	Attacks of model and driven in PV farms	Blockchain algorithm to address cyberattacks in software and cyber networks. Analyzed multiscale system modeling, event-trigger control, AI application, and hot patching.	Communication, sensor networks, and detection techniques.
[37]/2020	No	yes	yes	DOS, MITM, FDIA, Intrusion attack	No	Summary of IEC 61850 message structures and related cybersecurity concerns	Detection methods and sensor measurements
[38]/2022	yes	yes	yes	Attacks on CIA model.	Limited approach	Defined protected protocols and standards, cryptographic and authentication, intrusion prevention, education, access control, and required cybersecurity policy approaches.	Detection techniques of ML techniques

A comparison between existing review/survey papers on similar topics is described in Table 1, accordingly, the novel contribution and motivation of this paper are as follows:

- We have provided the overview of a cyber-attack on smart energy systems, a thorough description of the features, conceptual model, sensor and communication components, network protocols, and various cyber-attack types.
- The preceding study review models are summarized by using complex network theory, power network equations, system state equations, and data-driven methodologies taking into account the factual context of the CPSs link and the mismatch between research goals and quantitative indicators. They may describe the operational state of the energy grid, analyze load or line overload conditions, describe the fault mechanism, and predict/identify abnormal conditions. Moreover, this classification provides the network architecture and how to enhance the system's cyber-physical security. Considering these key points, suggestions from the previous review papers and we continued the survey in cyber-attack detection and mitigation.
- The primary contribution of this survey to the existing literature is that it attempts to investigate FDIA in smart grids and detect it by using unsupervised learning techniques. To realize the detection of cyber-attacks in the smart grid, first, we should understand the overview of the smart grid's architecture and the key points of grid attacks. Therefore, we have considered the literature on network architecture, FDIA attacks, types of detection, etc. We looked at a variety of cyberattack detection techniques such as replay, DOS, stealthy, and FDIA and concluded that unsupervised learning algorithms are better at spotting FDIA in smart grids for huge unlabeled data. We reviewed FDIA from a system-theoretic perspective, which more clearly demonstrates conceptual parallels and common operating principles. For example, we have shown how concepts gained from analyzing specific attacks that target different parts of the network, or how attack schemes can be combined to develop more malicious activities.
- For reliable and quick detection of stealthy FDIA in smart grids without the requirement for knowledge of network parameters or measurement distributions, we offer an unsupervised data mining approach. The algorithm is developed online after being offline-trained. This algorithm identifies a cyber-attack even when there is a significant amount of class mismatch, a sudden increase in data transfer in the network, and abnormalities in the system. This method can still operate well without experiencing any performance reduction because they do not have any set pattern or context. To the best of our knowledge, and in contrast to the aforementioned surveys, our work is the first to examine the features of smart grid security using unsupervised ML approaches and security metrics.

- Finally, the prospects and challenges of cyber-physical smart grids in the future are examined, which may help to clarify the cyber-physical security concerns that the next-generation smart grid must resolve.

3. Network Architecture under Cyber-Attacks in Smart Grids

Dispatcher sources, power electronic converters, communication cables, and loads make up the physical layer. System hardening can be used to take preventive action against physical layer threats. The communication channels that are bridged among the sources to enable data transfer make up the cyber layer. To save money by avoiding the costs associated with a fully connected communication infrastructure, networked converters display sparsity in their cyber-connections. A centralized approach necessitates considerable computation and communication over a wide geographic area. This prerequisite makes the centralized control strategy unworkable. Again, a fully decentralized control solution is not feasible due to the requirement of a very tight coupling between the unit operations. The key benefit of decentralized control is that it allows for the incorporation of various DG units into the microgrid without requiring any adjustments to the controller settings. However, in this instance, coordination must be sufficiently robust. The system's units cannot be coordinated to a sufficient degree using local variables [39]. To solve these problems, the installation of secondary, primary, and tertiary controllers in a hybrid cyber-layered microgrid with n parallel bidirectional converters and an equal power rating is shown in Figure 2. The cyber layer is represented by red arrows, and the physical circuit is represented by black lines. In a microgrid, the load is typically distributed across the converters at the primary control level, which is typically drooped control. On the other hand, the secondary control level lessens the steady-state inaccuracy caused by the droop control, while the tertiary level is in charge of energy export or import for microgrids. The distributed control topology has advantages over the centralized control topologies, including lower communication needs, lower computation burden, better scalability, good reliability, and better resilience.

The operating mode for each converter is either voltage or current-controlled. Primary layer control actions are independent of the communication system since local controllers are directly connected to converters. To enhance the performance of the sources' coordination, cooperative secondary controllers are used. A distributed communication layer, which only exchanges information with nearby units, enables these controllers. To accomplish secondary control goals, such as average voltage regulation and proportionate current sharing, each unit, represented as an agent in the cyber layer, sends and receives DC/AC voltage and current from the nearby agent(s). Tertiary control operates power management, energy management, system optimization, and economic dispatch as the highest level in the hierarchical design. Using a local converter and a digital communication link-based coordinated control system, such as a cutting-edge cloud-based communication platform, which has control bandwidths that are at least an order of magnitude apart, simultaneously allows for the implementation of hierarchical control. As the time scale lengthens and the level of control shifts from primary to tertiary, the control bandwidth contracts [40].

On a communication graph with an adjacency matrix, each converter broadcasts $I_i(t)$ and/or $V_i(t)$ to the DG units that are close by. Each analog voltage and current measurement from each converter is transmitted to its nearby control units utilizing a USB in conjunction with the Modbus protocol to carry out scattered, undirected communication. It is a technique for information transfer between electronic devices through serial lines. Signals from instrumentation and control devices are often transmitted using Modbus back to the main controller or data collection system. The simplest configuration would be connecting the serial ports on two machines, a client and a server, using a single serial cable. Each bit of the data is conveyed as a voltage, and the data are sent as a succession of ones and zeroes. Zeroes are sent as positive voltages and ones as negative. These voltage and current measurements will be collected from the Remote Terminal Unit (RTU) from the sensors. Telemetry Devices consist of RTUs and Master Terminal Units (MTUs). The RTUs

collect telemetry data from sensor components (distributed across domains), and MTUs, receive and process that data for management and topology manipulation (connected to core systems). This promotes efficient power generation and transmission.

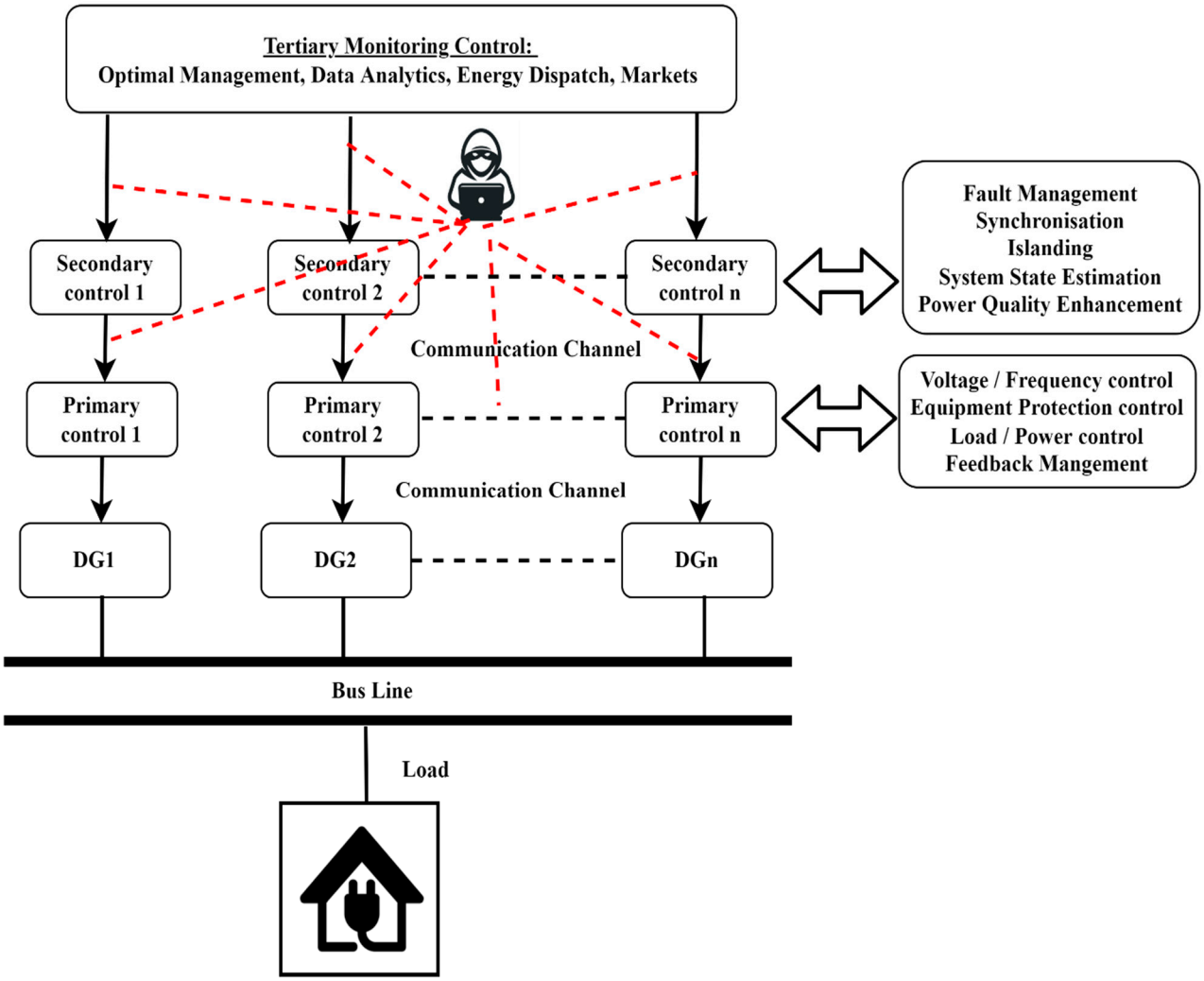

Figure 2. Hierarchal power sharing control building blocks in microgrids during a cyber-attack.

The current electricity grid is becoming more vulnerable, mostly because it develops and adopts new technologies such as telemetry devices and the Internet of Things (IoT). Additionally, recent research and publications show an increase in cyber security incidents and threats related between telemetry systems, SCADA, IoT, and the electric power grid [41]. Smart Grid is monitored and managed by a SCADA system that collects consumption statistics and behavior using IoT devices and Advanced Metering Infrastructure (AMI). By enabling two-way communication inside the system's infrastructure, using wireless communication networks improves the efficiency of electricity generation and delivery. To implement an effective generation and distribution plan, the generating centers have access to real-time data on power demand due to the association of smart meters and sensors across the power grid network [42]. As a result, the infrastructure of the power system has benefited considerably from the integration of these technologies, increasing energy efficiency and lowering electricity costs.

Real-time data from the electrical power grid are monitored, measured, and analyzed via SCADA, a type of process control system [43]. While it can ensure both short-range and long-range communications, SCADA is most effective in large-scale environments. The RTU, MTU, and Human–Machine Interface (HMI) are the three primary components of

this system. RTU is a device made up of three units. Data acquisition is performed by the first unit, logic programs from the MTU are run by the second unit, and communication infrastructure development is mostly handled by the third unit [44]. The MTU, which is a device for controlling and monitoring the RTU, is another component of SCADA. HMI is regarded as the final component of SCADA and serves as the operator's Graphical User Interface (GUI).

Over time, a few protocols were created to offer smart grid systems secure and dependable communication. Several industrial communication protocols used inside SCADA are Modicon Communication Bus (Modbus), Distributed Network Protocol version 3 (DNP3), Process Field Bus (Profibus), and International Standard Defining Communication Protocol 61850 (IEC61850). Smart meters, home appliances, and AMIs all communicate with one another via different communication protocols. Their vulnerabilities and intrinsic security requirements differ greatly [45,46].

While using two separate communication mediums, namely wired and wireless, new communication and information technologies with current intelligent monitoring systems play a crucial role in securing data transmission between smart meters and utilities. The advantages of wireless communications over wired communications include lower infrastructure costs and more robust connections in remote areas. Wireless technologies include Zigbee, Z-wave, WiMAX, Wi-Fi, DASH7 (D7A), cellular, and satellite. PLC is a wired communication that supports high-speed data from one device to another. It is suitable for some applications, such as smart metering, home automation, and lighting.

To guarantee end-to-end data transmission, the Transmission Control Protocol/Internet Protocol (TCP/IP) was initially applied in the smart grid. Due to its complex memory management issues and the fact that it is only appropriate for broad-area networks, this protocol is not thought to be a good choice for smart networks.

The Wide Area Network (WAN), Neighborhood Area Network (NAN), Home Area Network (HAN), Building Area Network (BAN), and Industrial Area Network (IAN), are all parts of the smart grid's communication architecture. Each NAN has a Control Center (CC) that is designed to handle its own. Building gateways track electricity use and client needs, which they subsequently send to the CC. Customers can alter their electricity usage and further energy conservation measures at any time to the CC, which saves both cost and energy. In the context of the smart grid, the security and privacy of information exchanges between customers and the CC have emerged as crucial and difficult issues. The man-in-the-middle, DDOS, impersonation, FDIA, brute-force, and replay attacks are just a few of the malicious assaults that the smart grid is susceptible to. These attacks have the potential to have a substantial negative impact on society. As a result, a security protocol should be provided in the smart grid.

The hierarchical architecture of the smart grid according to Figure 2, which has a limited number of sub-networks, is seen to be crucial in the infrastructure since it connects a wide range of systems; nevertheless, each sub-network is only in charge of a single geographic area. According to Figure 3, the smart grid network is divided into three primary sub-networks: WAN, NAN, and HAN. The additional sub-networks of WAN and NAN are Local Area Networks (LAN) and Field Area Networks (FAN). Industrial Area Network (IAN) and Building Area Network (BAN) are the two sub-networks that comprise FAN. PAN is a subnetwork of either IAN or BAN or HAN. Most of the research in FDIA primarily concentrates on four vulnerable protocols, including Modbus, DNP3, Profibus, and IEC61850, which are employed in the infrastructure of smart grids [47–49]. The expected communication network which includes RTU, MTU, smart meters, communication protocols such as Zigbee, Z-wave, WiMAX, etc., IoT, WAN, LAN, NAN, FAN BAN, IAN, HAN, and PAN established in the microgrid is shown in Figure 3.

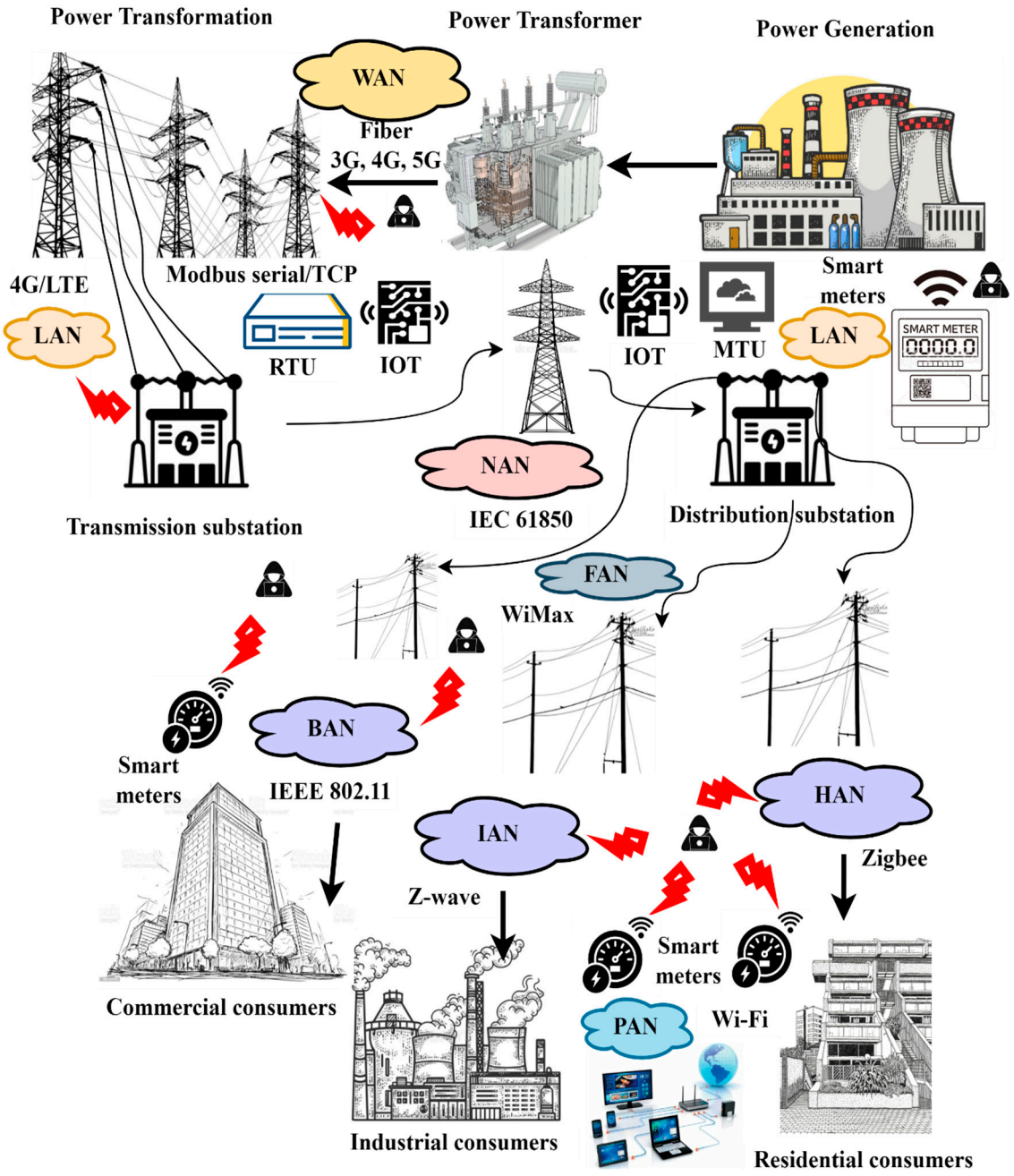

Figure 3. The basic network architecture of DG microgrid system.

4. FDIA Attack on Smart Grids

An Industrial Control System (ICS) is a special type of CPS that incorporates physical industrial process systems and facilities as well as SCADA systems, smart sensors, the industrial internet of things (IIOT), networked systems, and data analytics. The extensive use of sensors, networked devices, and SCADA to reduce voltage deviations, assess the network voltage profile, and provide appropriate voltage/current references is a result of the rapid organization of digitalization and growth of CPS. Situational awareness of cyber invasions and resistance to cyber-attacks are both present and developing security needs are expanding to incorporate both resilience to cyber-attacks and situational alertness of cyber intrusions. ICS systems are organized safety and high-value critical systems [50]. Security concerns are acknowledged as a major issue for CPSs, where both physical and cyber-attacks and defects could significantly affect how stable and secure a PV power

system operates. Regarding the security of CPS, confidentiality, integrity, and availability are three essential characteristics that must be safeguarded [51]. The disclosure, disruption, and deception attacks are three types of DDD attacks that can be used to categorize the attack models of CPSs. Attacks on disclosures might result in the release of confidential information. There are different types of cyber-attacks. For instance, denial of service (DoS), replay, jamming, random, topological, overloading, resonance, FDIA, Man in the middle, stealthy, etc., can be considered cyber-attacks. The commonly used cyber-attacks in DC/AC microgrids are DoS, FDIA, and replay attacks. DoS tries to make the communication network completely unavailable in the microgrid. Attacks that prevent users from using information are referred to as disruption assaults are DoS attacks. Replay attacks are another type of cyber-attack to record the reading of sensors for a certain amount of time and after that, repeat these readings in the system to deceive the operator. FDIAs, for example, include deception attacks to corrupt real data [52]. The various systems and layers of the smart grid can use FDIA. Four categories—physical, network, communication, and cyber—could be used to group them. Attacks on monitoring, control, and protection systems are included in physical-based FDIA. The communication-based FDIA gives a thorough analysis of the various communication methods used in smart grids and the risks that go along with them. If the attacker gains access to any network node, network FDIA is possible from anywhere. Cyber-based attacks are extremely harmful since they affect the system much more severely. These assaults occur when the adversary gains access to the control system or any applications connected to it, such as forecasting, estimating, economic dispatching, and trading in energy.

FDIA is regarded as a remote access intrusion since it alters the payloads of packets, compromising their data integrity [53]. Attackers use FDIA to obtain access to crucial ICS processes or process parameters and force them to carry out a freshly injected command or code. In cyber-physical systems, the term "FDIA" refers to a class of cyber-attacks where the goal is to alter the integrity of the network by manipulating some sensor devices and transmitting false data readings to the controller. The physical equipment affected by this attack includes switches for VSI, filters, active/reactive power controllers, and MPPTs. It also damages the electrical grid. System monitoring is necessary to ensure the power network operates dependably, and state estimation is a result of such monitoring to give attackers the most accurate assessment of the power grid.

False Setting Injection (FSI) and false command injection (FCI) are the two main forms of cyber-physical attacks that are highlighted in the literature that is currently available [54,55]. These attacks all impact system behavior, loss of inverter process control, current controller set points, device connection, and configuration. The FSI takes into account the hardware and software management of overcurrent, differential, and distance relays. The aforementioned ideas offer FSI protection utilizing local end data, but they are unreliable in a hybrid data and physical attack scenario. In the event of FCI attacks, proposals such as [56,57] offer the creation of attack models and system vulnerability analysis. A vulnerability known as a "command injection" allows an attacker to take control of one or more commands that are being executed on a system. Without the need to inject malicious code, command injection expands an application's normal capabilities by allowing it to deliver commands to the physical system shell.

FDIA can be modeled mathematically as in Equation (1),

$$FalseData = D_{i,j} + F_{i,j} \tag{1}$$

where $D_{i,j}$ is the original dataset, and $F_{i,j}$ is the injected data. The amalgamation of injected data with original data generates false data. Here, $F_{i,j}$ can be any of the following:

- Deletion of data from the original dataset, $D_{i,j}$
- Change of the data in the original dataset, $D_{i,j}$
- Addition of fake data to the original dataset, $D_{i,j}$

Although the representation in Equation (1) considers the data to be structured, the false data injection attacks can also be considered for unstructured data.

State estimate is essential for linking measurements obtained through the communication network and managing the operational activities in a smart grid. The SE automatically removes the faulty information brought on by random interferences, estimates or predicts the system operating state, and uses the redundancy of a real-time measurement system to increase data accuracy [58]. Using real-time information gathered from measuring devices such as PMU as depicted in Figure 4, SE aims to estimate the smart grid's operational conditions. Bus voltage, active and reactive power injections at each bus, and complex power flow on branches are examples of typical measurements.

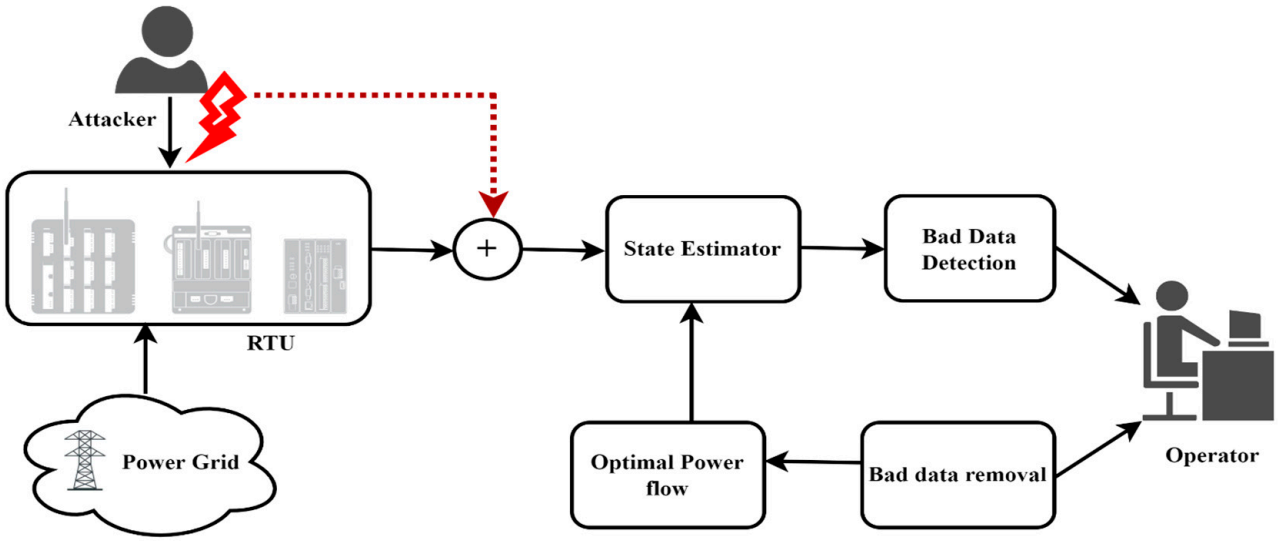

Figure 4. State estimation under Cyber-attack in smart grid.

The state vector for a system with n buses is represented as follows:

$$v = [v_1,\ v_2,\ v_3 \ldots\ldots v_n]^T\ \ (v_i \in R) \tag{2}$$

where v_i indicates the state variable at the ith bus, usually includes the voltage angle or voltage amplitude. Consider the measurement vector z. The measurement vector for a system with n buses is written as

$$z = [z_1,\ z_2,\ z_3 \ldots\ldots z_n]^T\ \ (z_i \in R) \tag{3}$$

There are some differences between measurement function values and actual measurement values for non-ideal sensors. State estimate in the actual electric power system, accounting for measurement errors, can be defined as:

$$z = \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_m \end{bmatrix} = \begin{bmatrix} H_1(v_1,\ v_2,\ v_3 \ldots\ldots v_n) \\ H_2(v_1,\ v_2,\ v_3 \ldots\ldots v_n) \\ \vdots \\ H_m(v_1,\ v_2,\ v_3 \ldots\ldots v_n) \end{bmatrix} + \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{bmatrix} \tag{4}$$

The relationship between system states v and measurements z can be created as a linear model using the DC power flow model, as shown below:

$$z = Hv + e \tag{5}$$

where e is the measurement error (additive noise) vector that is typically represented by the Gaussian distribution, v contains the voltage amplitude and voltage phase angle at the buses, z is the vector of measurements, and H is a Jacobian topological matrix that maps the system states to the measurements.

Where $H = \frac{\partial H(v)}{\partial v}$ is an invariable Jacobi matrix that depends on the impedance of the network topology. These issues are frequently resolved using the Weighted Least Squares algorithm. A quadratic optimization problem is created from the state estimation form, and the estimated linearized state vector v' is given by

$$v' = \left(H^T H\right)^{-1} H^T z \tag{6}$$

Bad data are produced as a result of measurement errors that happen at random, whereas false data are created knowingly by malicious attackers. SE, is a common method for detecting faulty data, is inefficient for detecting FDIA but excellent for detecting bad data. FDIA allows for the malicious injection of the generated data b into the power flow measurement vector as

$$Z_{bad} = Hv + b + e \tag{7}$$

and the injected false data vector is

$$b = [b_1,\ b_2,\ b_3 \ldots\ldots b_m]^T \tag{8}$$

$$Z_{bad} = z + b \tag{9}$$

When there exist false data injected by some attackers, b will be a nonzero vector.

The estimation state variable v' will be changed into v'_F due to the injected false data and there is $v'_F = v' + c$, where c is an n dimensional and nonzero vector. Assuming that the injected data vector Z_{bad} equals Hv, b will be ignored by the traditional detection method as mentioned above. This is because

$$\|Z_{bad} - Hv'_F\| = \|z + b - H(v' + c)\| = \|z - Hv')\| \tag{10}$$

Measurement data will be reviewed to ensure maximum accuracy and faulty data will be removed. Traditionally, the 2-norm residual test is used to identify faulty data:

$$\|z - Hv\|^2 < \in \tag{11}$$

where $\in$ is the threshold for BDD. Bad data exist and should be eliminated before the next iteration if the measurement residual rises above the threshold. However, these conventional BDD techniques are unable to identify stealthy and intelligent attacks such as FDI.

Where $\hat{v_{bad}}$, $\hat{x}$, and b denote the estimated state vector under attack, perfect FDI attack, and injected attack vector, respectively. In this case, the derived measurement residual in both with and without malicious data b is equal. Therefore, $b = H(\hat{v} + c) - Hv$ which results in

$$\|z - Hv\|^2 = \|Z_{bad} - Hv_{bad}\|^2 + \Gamma \tag{12}$$

where Γ is an error term attributed to the state estimation that must remain within a certain threshold depending on the power system. A method of attack that meets the aforementioned requirement is said to be stealthy. Even if the attacker just has a limited understanding of the network topology, such a covert attack vector is always there [59]. As a result, the traditional residual-based BDD process in DC state estimation may be unable to identify FDIA that are skillfully created by adversaries who are already familiar with the grid, such as its network architecture H and estimated states $\hat{v}$.

Big data classification becomes a challenge when examining several combinations of natural and artificial disturbances using typical sequential mining techniques. Additionally, important characteristics of an efficient classification technique include the capacity to identify large-area attack situations and handle data inconsistency difficulties, and dimensionality issues.

5. Detection Techniques of Cyber Attacks in Smart Grid

IoT technologies are widely used in smart grids to track changes in the environment or physical situations. In particular, SE is a crucial IoT-based smart grid application. It is used in system monitoring to obtain the most accurate assessment of the condition of the power grid through a study of the meter readings and power system topologies. FDIA, on the other hand, poses a serious threat to SE because it is usually difficult to detect.

Artificial Intelligence (AI) category consists of various ML and DL, DM, evolutionary, and fuzzy logic methods to detect FDIA. Techniques to detect cyber-attacks that target smart grids can be mainly classified into four categories ML: supervised, unsupervised, semi-supervised, and reinforcement algorithms. The various cyber-attack detecting algorithms in the smart grid as shown in Figure 5.

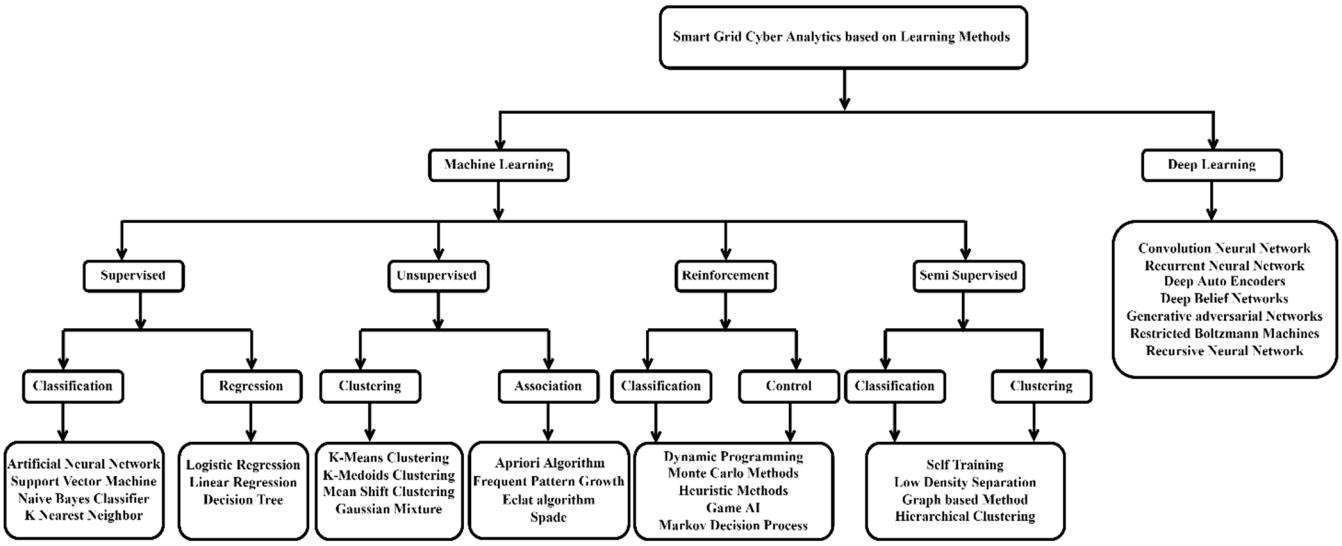

Figure 5. Cyber-attack detecting techniques in smart grid.

To minimize and identify FDIAs on SE in smart grids, some techniques have been proposed in the literature [60–63]. While the major objective of ML is to give the learning agent the ability to learn without guidance or human involvement, it might be seen as a potential example of ML in the future. The first kind of ML technique, supervised learning, assumes that the training data have been labeled and that the algorithm's output has already been input into the machine. The learning agent constructs a model to go from the input to the output, led by the training data, once it is aware of the output. The supervised learning techniques can be divided into Support Vector Machine (SVM), Artificial Neural Networks (ANN), Decision Trees (DTs), K-Nearest Neighbor (KNN), and Naive Bayesian Classifier (NB). Unsupervised learning, which belongs to the second group of ML approaches is computationally more expensive than supervised learning techniques but requires no labeling of datasets [64]. Unsupervised learning methods often focus on the following three objectives: (i) clustering, (ii) dimensionality reduction, and (iii) density evaluation. Principal component analysis (PCA), Dirichlet processes, K-means, and spectral clustering are a few examples of unsupervised ML. Between the supervised and unsupervised learning families, semi-supervised models use both labeled and unlabeled data for training. Algorithms used in reinforcement learning models use the estimated errors as rewards or deterrents. The most important features of reinforcement learning are trial-error search and delayed

reward. To maximize the desired performance, this family of models enables the automatic determination of the optimum behavior within a particular environment. Q-learning, Monte Carlo, and the Hidden Markov are illustrations of a model that fits inside this family.

Because the dataset's observations are all unlabeled and the algorithms learn the inherent structure from the input data, researchers are now advised to utilize unsupervised algorithms in smart grids to identify cyber-attacks [65,66]. The supervised technique has a high computing cost and necessitates measurements with labels from continuous samplings that may not be available in real-world operations. The majority of ML algorithms now in use for identifying FDIAs, including [67,68], are supervised and assess anomalous data that deviates in some way from the labeled data made available during training. Due to high labeling costs, the datasets gathered from real-world cyber-physical systems are only partially labeled [69]. Additionally, in practice, the scale of unlabeled data is typically much larger than that of labeled data, and these enormous amounts of unlabeled data infrequently participate in the supervised learning process. This absence causes the loss of important data and, ultimately, the collapse of the process. Some newly discovered cyberattack data are inherently unlabeled, making it challenging for supervised or semi-supervised learning to identify FDIA. To detect unobservable attacks or outliers that avoid the traditional BDD method, this research describes a new learning-based FDIA detection algorithm. This unsupervised learning technique can be used online and can identify these threats in milliseconds. The following sections describe ARM and clustering, which are two main categories for unsupervised algorithms. ARM is about finding relationships between the attributes of those data points and is the process of measuring the degree of association between any two items. On the other hand, clustering is about the data points and the process of segregating a huge number of data points into small groups sharing similar characteristics.

5.1. Association Rule Mining (ARM)

To be more advantageous, association rule learning, a form of unsupervised learning technique, looks for the dependence of one data item on another data item and maps accordingly [70]. It looks for any relevant relationships or correlations between the dataset's variables. It is built on various rules to find the significant relationships between database variables. Although data-mining techniques have some advantages, they can occasionally be used to detect FDIA in a smart grid since they only occasionally require high computational complexity depending on the data quantity. To improve outage diagnosing, this paper presents an ARM method to extract rules that help to find faulty pieces of equipment and identify FDI attacks [71,72]. To do this, three different datasets are processed and combined to gain useful features. This dataset includes the outage dataset, sub-transmission substation hourly load recorded by smart meters, and weather historical data. After the preprocessing section, the outage classes are labeled according to the malfunctioning piece of equipment. For every equipment-related outage cause, we form a dataset in which the record is labeled as either the main class or others depending on the main outage cause. After balancing the particular ARM algorithm is run and the obtained rules are evaluated using confidence, support, and lift to filter important rules. Support represents the percentage of things in a database that satisfy both the physical and its cyber-attack, whereas confidence represents the proportion of items that satisfy both the physical and its cyber-attack. Figure 6 depicts the process for finding a cyberattack that has affected the smart grid.

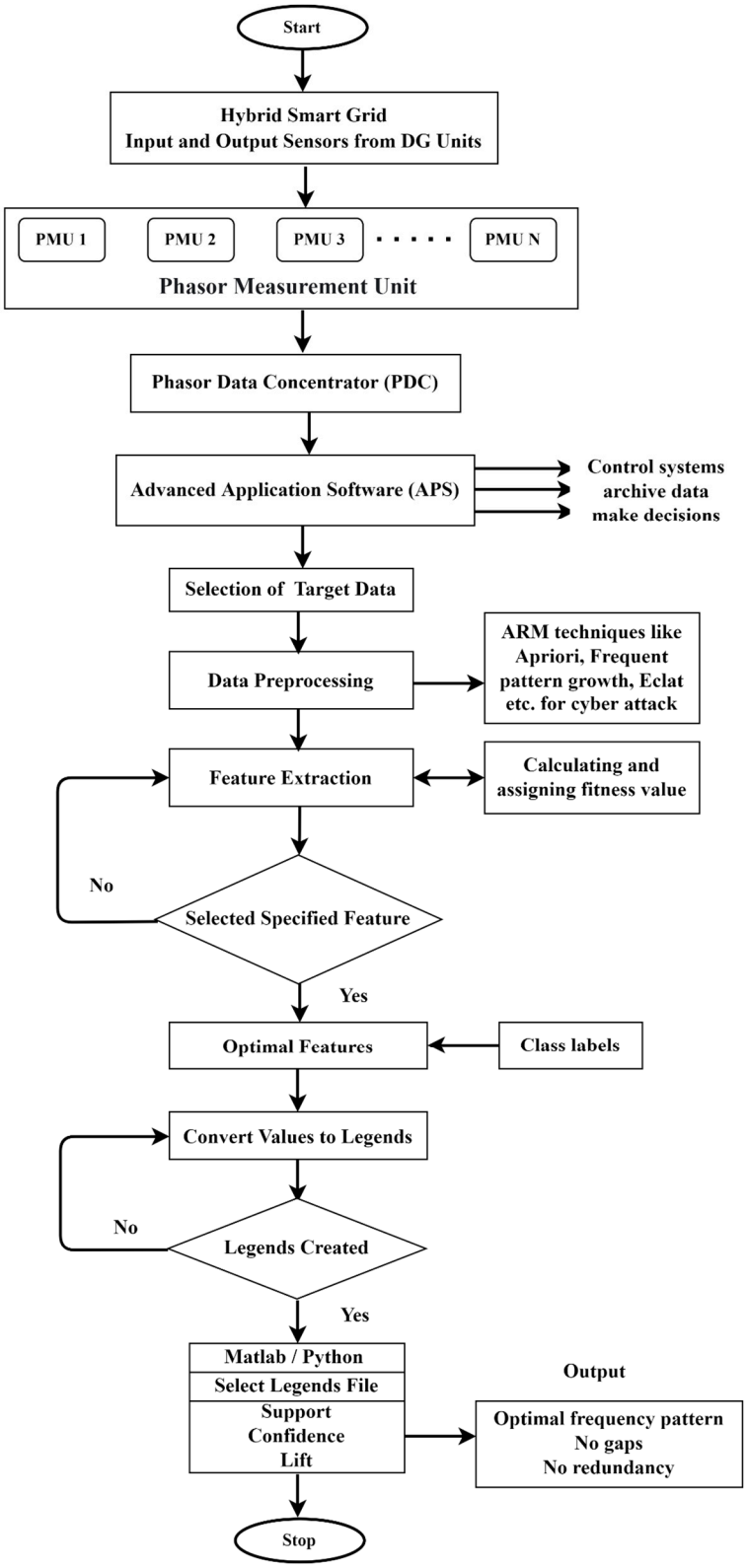

Figure 6. Flow chart of detecting cyber-attack based on ARM.

Smart meters, MTUs, RTUs, PDCs, and other devices will be sensing the high volume of current and voltage produced by DG units. This dataset must include both invasion and attacked signals. The sequential selection, preprocessing, transformation, data mining, interpreting, and evaluating database procedure used in this study makes use of the knowledge discovery database. Data cleaning is the process of eliminating noisy and useless

data from a collection. The term data integration refers to the combining of heterogeneous data from various sources into a single source, such as the fact that the same attacks occurred repeatedly in the same DG. The extract-load-transformation method is used for data integration. Data selection is the process by which data from the data collection, such as FDIA, plug or play, communication latency, load change, and link failure, that are determined to be pertinent to the analysis are chosen and retrieved. Data transformation is the process of converting data into the format needed for mining operations, such as values or legends. A method used to extract potentially relevant patterns is known as data mining. Identification of strictly increasing patterns that indicate knowledge based on predetermined metrics is the definition of pattern evaluation. The term knowledge representation refers to a method for visualizing data mining outcomes such as support, lift, and confidence. The data mining outcomes were calculated by using the following method.

Training historical datasets are a primary goal of DM methods in this study [73]. Finding interesting rules from transactional databases was the original purpose of ARM. A relationship between various attributes is described by an association rule: $If\ (A\ AND\ B)$ then (C). Following this criterion, C must also be present wherever A and B are. A given the relationship's frequency in the data can be determined via metrics for association rules. The conditional probability of C given A and B is the confidence, while the support is the prior probability of A, B, and C. It finds frequent sets of items (i.e., combinations of items that are purchased together in at least N transactions in the database), and from the frequent items sets such as $\{X, Y\}$, generates association rules of the form: $X \rightarrow Y$ and/or $Y \rightarrow X$.

Multiple algorithms, including Apriori [74], FP-Growth association rule [75], Eclat [76], Prefixspan [77], and Spade [78], are included in the ARM approach. For instance, Agarwal and Srikant [79] proposed the Apriori method in 1994. To extract common item sets (candidate generation) from a dataset, a level-wise bottom-up strategy is used. According to the required minimum support count, it locates the item sets. Apriori does have some restrictions, though. For instance, several scans are necessary. Each data set requires an explicit scan, which could result in I/O expenses. The existence of all necessary patterns is not guaranteed. Due to the requirement for extensive storage and processing time, the computational cost is likewise considerable.

The other method used frequently to mine the entire set of frequent patterns is pattern fragment growth (FP-Growth ARM). This methodology employs a divide-and-conquer strategy to establish a connection between various elements. The processing speed is relatively quick, and it makes greater use of the available space. When the patterns are paired and the dataset contains a lot of objects, this strategy is ineffective. The full set of patterns in sequential pattern mining is mined using Prefixspan (also known as Prefix-projected Sequential pattern mining). Candidate sequel generation efforts are far fewer than those for FP-Growth. It employs the divide and conquers strategy to unearth hidden patterns in the database. Prefixspan's drawbacks include the processing need for additional child patterns and gaps. However, since we would need to identify malicious patterns in real-time IoT traffic, these algorithms do not work well in network security applications. The SPADE algorithm makes use of the vertical ID-list format, which enables the creation of patterns and the computation of support for each sequence without engaging in an excessive amount of database reading that could burden the system. However, the SPADE algorithm has a problem that results from the generate-candidate-and-test methodology. This method might produce many sequence patterns that do not appear in the database very frequently. SPADE is a SNORT plugin and it minimizes computational and I/O costs by reducing database scans.

5.2. Clustering

The clustering approach is a typical matrix-theory-based unsupervised data-driven method. To put it another way, clustering is a technique used to divide up dissimilar data into many clusters while grouping like data into a single cluster. AMI offers network

interoperability and communications in an open environment, but it is susceptible to data integrity attacks, a common kind of cyberattack in the smart grid. Existing research has revealed that the adversary could attack the AMI with data integrity assaults by inserting altered and false data, leading to energy loss, power outages, welfare losses, infrastructure damage, and other problems [80–84]. Designing and creating efficient detection systems to lessen data integrity assaults in the AMI is therefore a primary issue. Data analysis methods such as association and supervised algorithms are the foundation of the majority of the detection schemes used to stop data integrity assaults [85]. Regression, prediction, and classification algorithms rely on the historical data that smart meters transmit, and they are sensitive to huge data set fluctuations that produce a broad range of normal data and low detection accuracy. As a result, there is a strong likelihood that the malicious data introduced by adversaries will go undetected. Therefore, it is essential to create a detection method that can overcome the aforementioned restrictions and is appropriate for real-world use. When data volatility is high, clustering is one of the methods that can achieve a high detection accuracy without relying on either predefined thresholds or external information.

Using cluster analysis, it is possible to show odd patterns of activity and identify assaults that would not be picked up by studying a single point by grouping together similar or related data points that are present throughout the network. Attacks that might otherwise go unnoticed can far more easily be found by analyzing groups of related actions. Without depending on signatures, explicit descriptions of attack classes, or labeled data for training. The goal of clustering algorithms is to divide the provided unlabeled data into clusters that achieve high inner similarity and outer dissimilarity. The input data can be clustered using a variety of techniques, including the well-known K-means [86], K-Medoids [87], Gaussian mixture model (GMM) [88], and Density-based Spatial Clustering of Applications with Noise (DBSCAN) methods [89].

K-means clustering is straightforward, effective, and widely used in the data mining industry. It is a signal processing-based vector quantization technique. Its flaw is that it randomly chooses K points at the beginning to serve as the cluster centroids, making it simple to get stuck in the local optimum. K-means clustering is a fast and robust algorithm and provides good results when the data are well separated. It calculates the square distance between the k numbers of centroids and an object; the object is assigned to the cluster of the nearest centroid. As a result, it is critical to identify objects that behave similarly near neighborhoods when under an FDI attack [90]. A K-means variation is more resistant to noise and outliers than K-Medoids clustering. K-Medoids employ a real point in the cluster to represent the cluster center rather than the mean point. It looks at cluster heads whose overall dissimilarity to all other cluster objects is the smallest [91]. Due to its efficiency in clustering data, DBSCAN has attracted attention for use in power systems to categorize measurement data. It is utilized for data measurement classification and gathering relevant input data sets before training, and it has not been fully taken into account in the online detection of FDI attacks on Microgrids. This problem is resolved by using a state observer to estimate converter voltage and current measurements, which are then provided to a well-trained ML model as inputs for the calculation of FDI attack vectors to update the state-space representation model [92]. Figure 7 depicts the flowchart for clustering-based cyber threat detection. The method utilized in ARM-based detection techniques for data selection, preprocessing, transformation, interpretation, and evaluation is the same. Attacked or normal data will have distinct distributions, which will lead to different cluster formations. In a feature space with adequate dimensions, these clusters would be recognizable. Additionally, a classifier can be trained to distinguish between the two groups such as attacked and normal, provided the data are supplied with class labels. When the size of measurement features grows along with an increase in the size of the power system, which results in more computing complexity, the curse of dimensionality becomes difficult to overcome. An ML classifier that can identify attacks on the dataset is then trained using the chosen best characteristics.

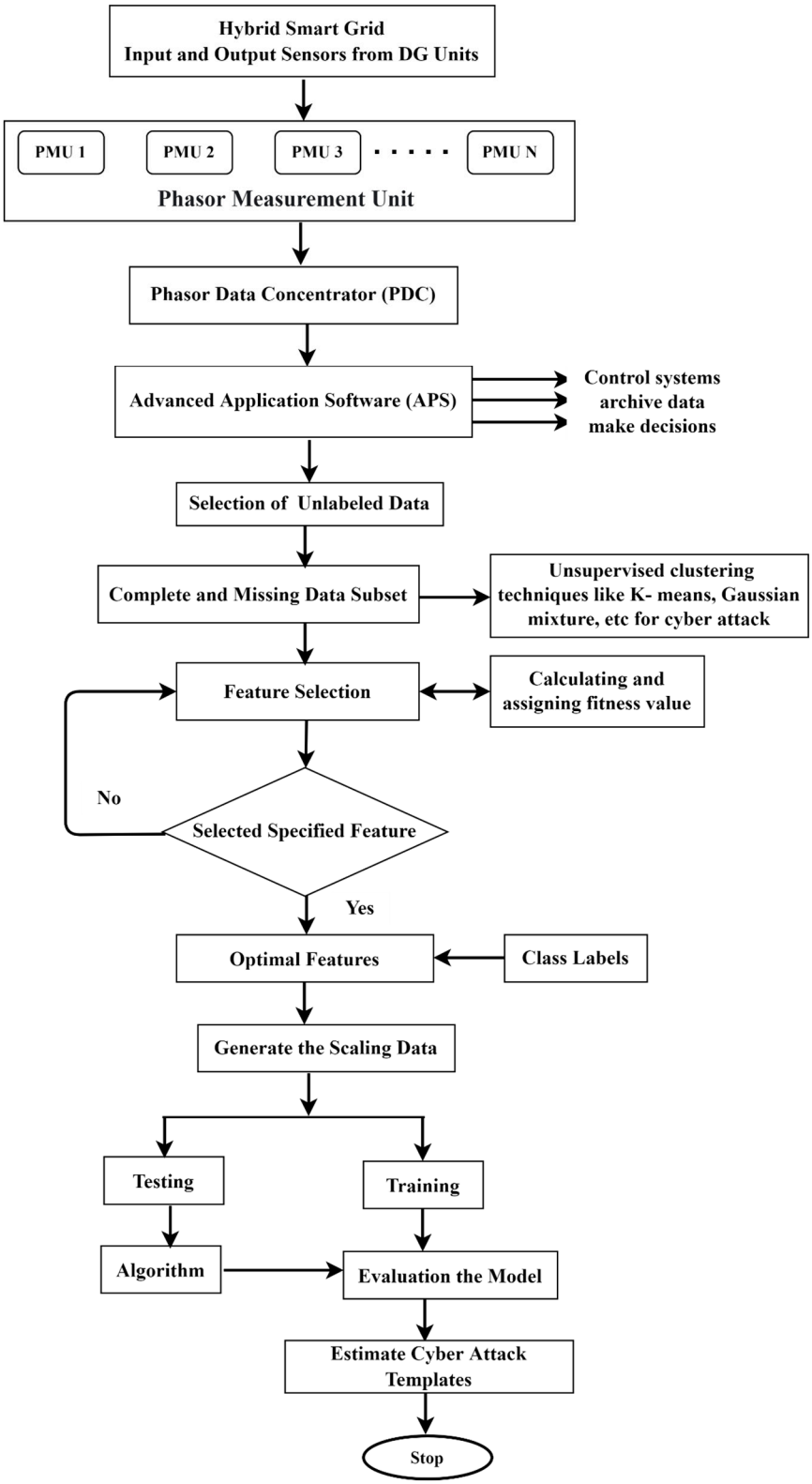

Figure 7. Cyber-attack detecting techniques in smart grid by using clustering.

6. Challenges and Future Generation

Some technical challenges must be overcome if cyber-resilient power systems are to become a reality. The problems and directions for the future are considered in the following few points.

The traditional grid and the smart grid are susceptible to human error. These mistakes may be the result of overworked personnel, which limits their ability to make decisions, or they may be the result of social engineering or insider attacks if workers are not prepared to deal with these types of assaults. Therefore, the smart grid would maintain service availability while providing several layers of security, utilizing the virtual private network (VPN) to increase secure communication during attacks.

Future CPS research should take into account the unpredictability of system parameters, modeling, observations, and the dynamic properties of smart grids, which are restricted by their varied states and operating conditions. The next generation of electrical systems will be completely dependent on the smart grid. Investigating and creating a standardized architecture, framework, and technology standard for the smart grid is crucial since it will serve as the basis for more suitable security regulations and remedies against cyberattacks.

The protocols that are currently being used would not offer very high security. With such outdated protocols, confidentiality, privacy, integrity, and responsibility can all be readily compromised. New security protocols are therefore required for smart grid networks. Depending on the needs of the smart grid application, a new protocol must be created or the existing protocol must be improved.

The absence of research interest in hybrid AC/DC smart grids or microgrids presents another difficulty for power system security. Future smart grids will likely combine AC/DC smart grids with DG power interfaces with load, energy storage, and power electronics converter grids. In a hybrid microgrid, the number of points of vulnerability to cyber exploitation has the potential to increase significantly because the CPS now includes various AC-based appliances in addition to the necessary protections against cyberattacks, which makes modeling, creating control strategies, and designing detection algorithms more challenging. Moreover, the control strategy for the hybrid grid, in addition to protecting their respective voltage regions, needs to consider AC/DC interlinking problem.

Before any cyberattack occurs, the models for AI-based detection systems must undergo significant training. As a result, strategies that identify not only incoming signals but also serve to both prevent new attacks and help in system recovery are required. In the field of power system control, a cutting-edge unsupervised ML application for CPS is emerging. To track the stability of CPS, it combines hybrid data from cyber and physical systems. Future research in cybersecurity is suggested to concentrate more on the model-free approach, either using an unsupervised or reinforcement detection method or enhanced SE that can assess the state of the system regardless of system dynamics. High-level security data structures and algorithms are required because the current state estimator methods cannot identify improper/defective data using the existing detection techniques present in the FDIAs.

Because intelligent grids connect many devices over extensive networks of geographic locations, this presents a problem. Protecting this equipment from the bigger infrastructure consequently becomes the main concern. A large amount of data from a power system requires fast and efficient computing, which has been a concern for several researchers. Task parallelism with multi-core, cluster and grid computing can reduce the computational time in an efficient data mining algorithm. Blockchain technology may help with future security issues brought on by bad nodes or hackers by enabling data sharing and encryption.

7. Conclusions

Smart grids integrate cutting-edge information and communication technologies into conventional power grids to provide and manage power efficiently. On the other hand, newly discovered security flaws in cyberspace could be used by potential adversaries to launch cyberattacks that cause enormous harm. An exhaustive analysis of the network architecture under cyber-attacks, state estimation in FDIA, and detection of FDIA by using unsupervised learning algorithms are presented in this research. Additionally, we reviewed occurrences of cyberattacks against smart grids that occurred globally between 2017 and

2023, taking into account a variety of factors such as attack type, detection, merits, and demerits. As a result, this article takes into account the limitations of the previous studies and offers a detailed analysis of potential attacks on smart grids as well as a comparison of various security measures. We analyzed and suggested a method based on unsupervised learning algorithms to detect cyber threats in smart grids using PMU and AMI metrics that connect the physical and cyber realms. Future research paths are thus presented from the standpoint of emerging technologies for the robust cybersecurity of smart grids against complex cyberattacks, as novel attack strategies are boundlessly exposed.

Author Contributions: Conceptualization, M.P. and S.J.P.; methodology, M.P. and P.S; validation, S.J.P., P.S. and M.P.; writing—original draft preparation, S.J.P.; writing—review and editing, P.S.; visualization, P.S.; supervision, P.S.; funding acquisition, P.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Acknowledgments: This work was supported by SERB, Department of Science and Technology, Government of India for the project file number SIR/2022/000299 through SIRE fellowship.

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

References

1. Abrahamsen, F.E.; Ai, Y.; Cheffena, M. Communication Technologies for Smart Grid: A Comprehensive Survey. *Sensors* **2021**, *21*, 8087. [CrossRef]
2. Pinto, S.J.; Panda, G. Improved Decoupled Control and Islanding Detection of Inverter-based Distribution in Multibus Microgrid Systems. *J. Power Electron.* **2016**, *4*, 1526–1540. [CrossRef]
3. Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D. A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements, and Challenges. *IEEE Commun. Surv.* **2013**, *15*, 5–20. [CrossRef]
4. Alanazi, M.A.; Mahmood, A.; Chowdhury, M.J.M. SCADA Vulnerabilities and Attacks: A Review of the State-of-the-Art and Open Issues. *Comput. Secur.* **2023**, *125*, 103028. [CrossRef]
5. Shi, L.; Dai, Q.; Ni, Y. Cyber-Physical Interactions in Power Systems: A Review of Models, Methods, and Applications. *Electr. Power Syst. Res.* **2018**, *163*, 396–412. [CrossRef]
6. Mohammadi, Z.; Pinto, S.J.; Panda, G.; Thokchom, S. A Survey of Cyber Security in Smart Microgrid. In *Sustainable Energy, and Technological Advancements*; Panda, G., Naayagi, R.T., Mishra, S., Eds.; Advances in Sustainability Science and Technology; Springer: Singapore, 2022.
7. Bo, X.; Qu, Z.; Wang, L.; Dong, Y.; Zhang, Z.; Wang, D. Active Defense Research against False Data Injection Attacks of Power CPS Based on Data-Driven Algorithms. *Energies* **2022**, *15*, 7432. [CrossRef]
8. Lai, S.; Chen, B.; Li, T.; Yu, L. Packet-Based State Feedback Control under DOS Attacks in Cyber-Physical Systems. *IEEE Trans. Circuits Syst. II Express Briefs* **2019**, *66*, 1421–1425. [CrossRef]
9. Kim, J.; Tong, L. On Topology Attack of a Smart Grid. In Proceedings of the IEEE PES Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 24–27 February 2013.
10. Antoniadis, N.; Cordy, M.; Sifaleras, A.; Le Traon, Y. Preventing Overloading Incidents on Smart grids: A Multi-Objective Combinatorial Optimization Approach. In *Optimization and Learning OLA*; Springer: Cham, Switzerland, 2020; Volume 1173, pp. 269–281.
11. Wu, Y.; Wei, Z.; Weng, J.; Li, X.; Deng, R.H. Resonance Attacks on Load Frequency Control of Smart Grids. *IEEE Trans. Smart Grid* **2018**, *9*, 4490–4502. [CrossRef]
12. Du, M.; Pierrou, G.; Wang, X.; Kassouf, M. Targeted False Data Injection Attacks against AC State Estimation without Network Parameters. *IEEE Trans. Smart Grid* **2021**, *12*, 349–5361. [CrossRef]
13. Costilla-Enriquez, N.; Weng, Y. Attack Power System State Estimation by Implicitly Learning the Underlying Models. *IEEE Trans. Smart Grid* **2022**, *14*, 649–662. [CrossRef]
14. Liu, Y.; Ning, P.; Reiter, M.K. False Data Injection Attacks against State Estimation in Electric Power Grids. *ACM Trans. Inf. Syst. Secur.* **2011**, *14*, 33. [CrossRef]
15. Heming, H.; Fei, L.; Tinghui, O.; Xiaoming, Z. Sequential Detection of Microgrid Bad Data via a Data-Driven Approach Combining Online Machine Learning with Statistical Analysis. *Front. Energy Res.* **2022**, *10*, 861563.
16. El Mrabet, Z.; Kaabouch, N.; El Ghazi, H.; El Ghazi, H. Cyber-Security in Smart Grid: Survey and Challenges. *Comput. Electr. Eng.* **2018**, *67*, 469–482. [CrossRef]
17. Hasan, M.K.; Habib, A.; Shukur, Z.; Ibrahim, F.; Islam, S.; Razzaque, M.A. Review on Cyber-Physical and Cyber-Security System in Smart Grid: Standards, Protocols, Constraints, and Recommendations. *J. Netw. Comput. Appl.* **2023**, *209*, 103540. [CrossRef]

18. Tufail, S.; Parvez, I.; Batool, S.; Sarwat, A. A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid. *Energies* **2021**, *14*, 5894. [CrossRef]
19. Amin, M.; El-Sousy, F.F.M.; Aziz, G.A.A.; Gaber, K.; Mohammed, O.A. CPS Attacks Mitigation Approaches on Power Electronic Systems with Security Challenges for Smart Grid Applications: A Review. *IEEE Access* **2021**, *9*, 38571–38601. [CrossRef]
20. Liu, Q.; Hagemeyer, V.; Keller, H.B. A Review of Rule Learning-Based Intrusion Detection Systems and their Prospects in Smart Grids. *IEEE Access* **2021**, *9*, 57542–57564. [CrossRef]
21. Abir, S.M.A.A.; Anwar, A.; Choi, J.; Kayes, A.S.M. IoT-Enabled Smart Energy Grid: Applications and Challenges. *IEEE Access* **2021**, *9*, 50961–50981. [CrossRef]
22. Nafees, M.N.; Saxena, N.; Cardenas, A.; Grijalva, S.; Burnap, P. Smart Grid Cyber-Physical Situational Awareness of Complex Operational Technology Attacks: A Review. *ACM Comput. Surv.* **2022**, *55*, 215. [CrossRef]
23. Ding, J.; Qammar, A.; Zhang, Z.; Karim, A.; Ning, H. Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions. *Energies* **2022**, *15*, 6799. [CrossRef]
24. Tuyen, N.D.; Quan, N.S.; Linh, V.B.; Van Tuyen, V.; Fujita, G. A Comprehensive Review of Cybersecurity in Inverter-Based Smart Power System Amid the Boom of Renewable Energy. *IEEE Access* **2022**, *10*, 35846–35875. [CrossRef]
25. Xu, Y. A Review of Cyber Security Risks of Power Systems: From Static to Dynamic False Data Attacks. *Prot. Control. Mod. Power Syst.* **2020**, *5*, 19. [CrossRef]
26. 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.
27. Liberati, F.; Garone, E.; Di Giorgio, A. Review of Cyber-Physical Attacks in Smart Grids: A System-Theoretic Perspective. *Electronics* **2021**, *10*, 1153. [CrossRef]
28. Alsuwian, T.; Butt, S.A.; Amin, A.A. Smart Grid Cyber Security Enhancement: Challenges and Solutions—A Review. *Sustainability* **2022**, *14*, 14226. [CrossRef]
29. Mohammadi, F. Emerging Challenges in Smart Grid Cybersecurity Enhancement: A Review. *Energies* **2021**, *14*, 1380. [CrossRef]
30. Yohanandhan, R.V.; Elavarasan, R.M.; Manoharan, P.; Mihet-Popa, L. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis with Cyber Security Applications. *IEEE Access* **2020**, *8*, 151019–151064. [CrossRef]
31. Zhang, H.; Liu, B.; Wu, H. Smart Grid Cyber-Physical Attack and Defense: A Review. *IEEE Access* **2021**, *9*, 29641–29659. [CrossRef]
32. Sridhar, S.; Hahn, A.; Govindarasu, M. Cyber-Physical System Security for the Electric Power Grid. *Proc. IEEE* **2012**, *100*, 210–224. [CrossRef]
33. Liang, G.; Zhao, J.; Luo, F.; Weller, S.R.; Dong, Z.Y. A Review of False Data Injection Attacks Against Modern Power Systems. *IEEE Trans. Smart Grid* **2017**, *8*, 1630–1638. [CrossRef]
34. Humayed, A.; Lin, J.; Li, F.; Luo, B. Cyber-Physical Systems Security—A Survey. *IEEE Internet Things J.* **2017**, *4*, 1802–1831. [CrossRef]
35. 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]
36. Ye, J.; Giani, A.; Elasser, A.; Mazumder, S.K.; Farnell, F.; Mantooth, H.A.; Kim, T.; Liu, J.; Chen, B.; Seo, G.-S.; et al. A Review of Cyber–Physical Security for Photovoltaic Systems. *IEEE J. Emerg. Sel. Top. Power Electron.* **2022**, *10*, 4879–4901. [CrossRef]
37. Hussain, S.M.S.; Ustun, T.S.; Kalam, A. A Review of IEC 62351 Security Mechanisms for IEC 61850 Message Exchanges. *IEEE Trans. Ind. Inform.* **2020**, *16*, 5643–5654. [CrossRef]
38. Khoei, T.T.; Slimane, H.O.; Kaabouch, N. A Comprehensive Survey on the Cyber-Security of Smart Grids: Cyber-Attacks, Detection, Countermeasure Techniques, and Future Directions. In *Cryptography and Security*; Artificial Intelligence; Cornell University: Ithaca, NY, USA, 2022.
39. Gaggero, G.B.; Girdinio, P.; Marchese, M. Advancements and Research Trends in Microgrids Cybersecurity. *Appl. Sci.* **2021**, *11*, 7363. [CrossRef]
40. Villalón, A.; Rivera, M.; Salgueiro, Y.; Muñoz, J.; Dragičević, T.; Blaabjerg, F. Predictive Control for Microgrid Applications: A Review Study. *Energies* **2020**, *13*, 2454. [CrossRef]
41. Sayed, K.; Gabbar, H.A. SCADA and Smart Energy Grid Control Automation. *Smart Energy Grid Eng.* **2017**, *18*, 481–514. [CrossRef]
42. Ferrag, M.A.; Babaghayou, M.; Yazici, M.A. Cyber Security for Fog-based Smart Grid SCADA Systems: Solutions and Challenges. *J. Inf. Secur. Appl.* **2020**, *52*, 102500. [CrossRef]
43. Huitsing, P.; Chandia, R.; Papa, M.; Shenoi, S. Attack Taxonomies for the Modbus Protocols. *Int. J. Crit. Infrastruct. Prot.* **2008**, *1*, 37–44. [CrossRef]
44. Kuzlu, M.; Pipattanasompom, M.; Rahman, S. A Comprehensive Review of Smart Grid Related Standards and Protocols. In Proceedings of the 2017 5th International Istanbul Smart Grid and Cities Congress and Fair (ICSG), Istanbul, Turkey, 12–16 April 2017.
45. Mackiewicz, R.E. Overview of IEC 61850 and Benefits. In Proceedings of the 2006 IEEE PES Power Systems Conference and Exposition, Atlanta, GA, USA, 29 October–1 November 2006.
46. Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P. A Survey on Smart Grid Potential Applications and Communication Requirements. *IEEE Trans. Ind. Inform.* **2013**, *9*, 28–42. [CrossRef]
47. Burg, A.; Chattopadhyay, A.; Lam, K.-Y. Wireless Communication and Security Issues for Cyber-Physical Systems and the Internet-of-things. *Proc. IEEE* **2018**, *106*, 38–60. [CrossRef]

48. Ahmed, S.; Gondal, T.M.; Adil, M.; Malik, S.A.; Qureshi, R. A Survey on Communication Technologies in Smart Grid. In Proceedings of the 2019 IEEE PES GTD Grand International Conference and Exposition Asia (GTD Asia), Bangkok, Thailand, 19–23 March 2019; pp. 7–12.
49. Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P. Smart Grid Technologies: Communication Technologies and Standards. *IEEE Trans. Ind. Inform.* **2011**, *7*, 529–539. [CrossRef]
50. Sengupta, J.; Ruj, S.; Bit, S.D. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [CrossRef]
51. Lopez, C.; Sargolzaei, A.; Santana, H.; Huerta, C. Smart Grid Cyber Security: An Overview of Threats and Countermeasures. *J. Energy Power Eng.* **2015**, *9*, 632–647.
52. Musleh, A.S.; Chen, G.; Dong, Z.Y. A Survey on the Detection Algorithms for False Data Injection Attacks in Smart Grids. *IEEE Trans. Smart Grid* **2020**, *11*, 2218–2234. [CrossRef]
53. Zhang, Y.; Wang, J.; Chen, B. Detecting False Data Injection Attacks in Smart Grids: A Semi-Supervised Deep Learning Approach. *IEEE Trans. Smart Grid* **2021**, *12*, 623–634. [CrossRef]
54. Hong, J.; Nuqui, R.F.; Kondabathini, A.; Ishchenko, D.; Martin, A. Cyber Attack Resilient Distance Protection and Circuit Breaker Control for Digital Substations. *IEEE Trans. Ind. Inform.* **2019**, *15*, 4332–4341. [CrossRef]
55. Qu, Z.; Dong, Y.; Qu, N.; Li, H.; Cui, M.; Bo, X.; Wu, Y.; Mugemanyi, S. False Data Injection Attack Detection in Power Systems Based on Cyber-Physical Attack Genes. *Front. Energy Res.* **2021**, *9*, 644489. [CrossRef]
56. Kleinmann, A.; Amichay, O.; Wool, A.; Tenenbaum, D.; Bar, O.; Lev, L. Stealthy Deception Attacks Against SCADA Systems, Computer Security. SECURE CyberICPS 2017. In *Lecture Notes in Computer Science*; Springer: Berlin/Heidelberg, Germany, 2018; p. 10683.
57. Rajesh, L.; Satyanarayana, P. Detection and Blocking of Replay, False Command, and False Access Injection Commands in SCADA Systems with Modbus Protocol. *Secur. Commun. Netw.* **2021**, *4*, 8887666.
58. Aeiad, F.; Gao, W.; Momoh, J. Bad Data Detection for Smart Grid State Estimation. In Proceedings of the 2016 North American Power Symposium (NAPS), Denver, CO, USA, 18–20 September 2016; pp. 1–6.
59. 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]
60. 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]
61. Chaojun, G.; Jirutitijaroen, P.; Motani, M. Detecting False Data Injection Attacks in AC state estimation. *IEEE Trans. Smart Grid* **2015**, *6*, 2476–2483. [CrossRef]
62. 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]
63. Ashok, A.; Govindarasu, M.; Ajjarapu, V. Online Detection of Stealthy False Data Injection Attacks in Power System State Estimation. *IEEE Trans. Smart Grid* **2018**, *9*, 1636–1646. [CrossRef]
64. Zhuang, P.; Deng, R.; Liang, H. False Data Injection Attacks Against State Estimation in Multiphase and Unbalanced Smart Distribution Systems. *IEEE Trans. Smart Grid* **2019**, *10*, 6000–6013. [CrossRef]
65. Aboelwafa, M.M.N.; Seddik, K.G.; Eldefrawy, M.H.; Gadallah, Y.; Gidlund, M. A Machine-Learning-Based Technique for False Data Injection Attacks Detection in Industrial IoT. *IEEE Internet Things J.* **2020**, *7*, 8462–8471. [CrossRef]
66. Vincent, P.; Larochelle, H.; Lajoie, I.; Bengio, Y.; Manzagol, P.-A. Stacked Denoising Autoencoders: Learning Useful Representations in a Deep Network with a Local Denoising Criterion. *J. Mach. Learn. Res.* **2010**, *11*, 3371–3408.
67. Yao, L.; Ge, Z. Scalable Semi-Supervised GMM for Big Data Quality Prediction in Multimode Processes. *IEEE Trans. Ind. Electron.* **2019**, *66*, 3681–3692. [CrossRef]
68. Bennett, K.P.; Demiriz, A. *Semi-Supervised Support Vector Machines, in NIPS*; The MIT Press: Cambridge, MA, USA, 1998; pp. 368–374.
69. Wilson, D.; Tang, Y.; Yan, J.; Lu, Z. Deep Learning-Aided Cyber-Attack Detection in Power Transmission Systems. In Proceedings of the IEEE Power Energy Soc General Meet PESGM, Portland, OR, USA, 5–10 August 2018.
70. Ju, C.; Bao, F.; Xu, C.; Fu, X. A Novel Method of Interestingness Measures for Association Rules Mining Based on Profit. *Discret. Dyn. Nat. Soc.* **2015**, *2*, 868634. [CrossRef]
71. Abu, M.S.; Selamat, S.R.; Yusof, R.; Ariffin, A. An Attribution of Cyberattack using Association Rule Mining (ARM). *Int. J. Adv. Comput. Sci. Appl. (IJACSA)* **2020**, *11*, 2. [CrossRef]
72. Lou, P.; Lu, G.; Jiang, X.; Jiang, Z.; Hu, J.; Yan, J. Cyber Intrusion Detection through Association Rule Mining on Multi-Source Logs. *Appl. Intell.* **2021**, *51*, 4043–4057. [CrossRef]
73. Wu, X.; Zhang, C.; Zhang, S. Efficient Mining of both Positive and Negative Association Rules. *ACM Trans. Inf. Syst.* **2004**, *22*, 381–405. [CrossRef]
74. Prakash, S.; Vijayakumar, M. An Effective Network Traffic Data Control Using Improved Apriori Rule Mining. *Circuits Syst.* **2016**, *7*, 3162–3173. [CrossRef]
75. Rosyid, N.R.; Ohrui, M.; Kikuchi, H.; Sooraksa, P.; Terada, M. A Discovery of Sequential Attack Patterns of Malware in Botnets. In Proceedings of the 2010 IEEE International Conference on Systems, Istanbul, Turkey, 10–13 October 2010; Man and Cybernetics, pp. 2564–2570.

76. Isam, K.T.; Osman, N.U.; Bayat, O.; Alsaedi, K.H. Improving IDSs Alerts to Improve High-Quality Network Security by using Data Mining Techniques. *Aurum J. Eng. Syst. Archit.* **2017**, *1*, 17–29.
77. Ohrui, M.; Kikuchi, H.; Rosyid, N.R.; Terada, M. Mining Botnet Coordinated Attacks using an Apriori-Prefix Span Hybrid Algorithm. J. Inf. Process. *J. Inf. Process.* **2013**, *21*, 607–616.
78. Nugroho, E.P.; Megasari, R.; Junaeti, E.; Pribadi, S.R. Implementation of CM-SPADE Algorithm in Building Denial of Service Detection System Model Using Snort. In Proceedings of the 7th Mathematics, Science, and Computer Science Education International Seminar, MSCEIS 2019, Bandung, West Java, Indonesia, 12 October 2019.
79. Agrawal, R.; Srikant, R. Mining sequential patterns. In Proceedings of the Eleventh International Conference on Data Engineering, Taipei, Taiwan, 6–10 March 1995; pp. 3–14.
80. Silva, C.; Faria, P.; Vale, Z. Clustering Support for an Aggregator in a Smart Grid Context. In *Hybrid Intelligent Systems*; Madureira, A., Abraham, A., Gandhi, N., Varela, M., Eds.; HIS 2018; Advances in Intelligent Systems and Computing; Springer: Berlin/Heidelberg, Germany, 2020; Volume 923.
81. Saddam, A.; Muhammad, I.; Ahmed, H.S.; Wu, J.; Nan, D.D.; Ahmad, S. Protection of a Smart Grid with the Detection of Cyber-Malware Attacks using Efficient and Novel Machine Learning Models. *Front. Energy Res.* **2022**, *10*, 1102.
82. Lei, W.; Xu, P.; Qu, Z.; Bo, X.; Dong, Y.; Zhang, Z.; Li, Y. Coordinated Cyber-Attack Detection Model of Cyber-Physical Power System Based on the Operating State Data Link. *Front. Energy Res.* **2021**, *9*, 666130.
83. Hussain, T.; Saeed, M.I.; Khan, I.U.; Aslam, N.; Aljameel, S.S. Implementation of a Clustering Based DDoS Detection Method. *Electronics* **2022**, *11*, 2804. [CrossRef]
84. Bohara, B.; Bhuyan, J.; Wu, F.; Ding, J. A Survey on the Use of Data Clustering for Intrusion Detection System in Cyber Security. *Int. J. Netw. Secur. Appl.* **2020**, *12*, 1–18. [PubMed]
85. Faisal, M.A.; Aung, Z.; Williams, J.R.; Sanchez, A. Data-Stream based Intrusion Detection System for Advanced Metering Infrastructure in Smart Grid: A feasibility study. *IEEE Syst. J.* **2015**, *9*, 31–44. [CrossRef]
86. Pena, J.; Lozano, J.; Larranaga, P. An Empirical Comparison of Four Initialization Methods for the k-Means Algorithm. *Pattern Recognit. Lett.* **1999**, *20*, 1027–1040. [CrossRef]
87. Jin, X.; Han, J. K-Medoids Clustering. In *Encyclopedia of Machine Learning*; Sammut, C., Webb, G.I., Eds.; Springer: Berlin/Heidelberg, Germany, 2011.
88. Sreenivasulu, V.; Prasad, R.S. A Methodology for Cybercrime Identification using Email Corpus based on the Gaussian Mixture Model. *Int. J. Comput. Appl.* **2015**, *117*, 29–32.
89. Farrokhifard, M.M.; Hatami, M.; Venkatasubramanian, V.M.; Torresan, G.; Panciatici, P.; Xavier, F. Clustering of Power System Oscillatory Modes using Dbscan Technique. In Proceedings of the 2019 North American Power Symposium (NAPS), Wichita, KS, USA, 13–15 October 2019; pp. 1–6.
90. Anwar, A.; Mahmood, A.N.; Zahir, T. Identification of Vulnerable Node Clusters against False Data Injection Attack in an AMI-based Smart Grid. *Inf. Syst.* **2015**, *53*, 201–212. [CrossRef]
91. Gallardo, J.L.; Ahmed, M.A.; Jara, N. Clustering Algorithm-Based Network Planning for Advanced Metering Infrastructure in Smart Grid. *IEEE Access* **2021**, *9*, 48992–49006. [CrossRef]
92. Abazari, A.; Zadsar, M.; Ghafouri, M.; Atallah, R.; Assi, C. A Data Mining/ANFIS and Adaptive Control for Detection and Mitigation of Attacks on DC MGs. *IEEE Trans. Smart Grid*, 2022; (*Early access*). [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.