applied sciences

MDPI

Review

A Review of Smart Grid Anomaly Detection Approaches Pertaining to Artificial Intelligence

Marcelo Fabian Guato Burgos [1,*], Jorge Morato [1] and Fernanda Paulina Vizcaino Imacaña [2]

[1] Department of Computer Science, Campus Leganés, Universidad Carlos III de Madrid, 28911 Leganés, Spain; jmorato@inf.uc3m.es
[2] School of Computer Science, Faculty of Technical Sciences, Main Campus, Universidad Internacional del Ecuador, Quito 170411, Ecuador; pvizcaino@uide.edu.ec
* Correspondence: 100390410@alumnos.uc3m.es; Tel.: +593-987270208

Featured Application: This review can be used as a guiding reference to how studies of distinct types of smart grid abnormalities are approached.

Abstract: The size of power grids and a complex technological infrastructure with higher levels of automation, connectivity, and remote access make it necessary to be able to detect anomalies of various kinds using optimal and intelligent methods. This paper is a review of studies related to the detection of anomalies in smart grids using AI. Digital repositories were explored considering publications between the years 2011 and 2023. Iterative searches were carried out to consider studies with different approaches, propose experiments, and help identify the most applied methods. Seven objects of study related to anomalies in SG were identified: attacks on data integrity, unusual measurements and consumptions, intrusions, network infrastructure, electrical data, identification of cyber-attacks, and use of detection devices. The issues relating to cybersecurity prove to be widely studied, especially to prevent intrusions, fraud, data falsification, and uncontrolled changes in the network model. There is a clear trend towards the conformation of anomaly detection frameworks or hybrid solutions. Machine learning, regression, decision trees, deep learning, support vector machines, and neural networks are widely used. Other proposals are presented in novel forms, such as federated learning, hyperdimensional computing, and graph-based methods. More solutions are needed that do not depend on a lot of data or knowledge of the network model. The use of AI to solve SG problems is generating an evolution towards what could be called next-generation smart grids. At the end of this document is a list of acronyms and terminology.

Keywords: smart grid; cyber physical systems; anomaly detection; artificial intelligence

Citation: Guato Burgos, M.F.; Morato, J.; Vizcaino Imacaña, F.P. A Review of Smart Grid Anomaly Detection Approaches Pertaining to Artificial Intelligence. *Appl. Sci.* **2024**, *14*, 1194. https://doi.org/10.3390/app14031194

Academic Editors: Cristian-Dragoș Dumitru, Gheorghe Grigoras and Subhas Mukhopadhyay

Received: 20 December 2023
Revised: 25 January 2024
Accepted: 30 January 2024
Published: 31 January 2024

1. Introduction

This study aims to examine the many solutions developed for detecting anomalies in Smart Grids (SGs). Specifically, it focuses on those solutions that employ artificial intelligence techniques or approaches. The objective is to gain insight into their practicality and highlight the prevailing trends in this area.

Digital technologies are being integrated into the foundational framework of the electrical grid. The driving forces behind this include the integration of renewable energy sources, ensuring the security of energy supply, and enhancing infrastructure operation and maintenance efficiency [1].

Smart grids face the following research challenges: (1) how to get a more accurate prediction method; (2) how to find optimal programming when an online learning task is performed; and (3) how to learn multiple tasks in a more automatic way [2]. As the complexity of the systems that support the operation of the power grids increases, there is also a growing need for a shift in the paradigm of network management from reactive to

proactive, and this can be achieved using advanced monitoring tools, data analysis, and predictive methods [3].

Future smart grids will require systems that can monitor, predict, schedule, learn, and make consumption decisions in real time that are highly associated with external weather conditions and energy output [2,4].

The relevance of detecting, localizing, and predicting abnormal energy network events or behaviors extends to customers, network operators, service providers, and regulatory bodies. The anomaly detection solutions are applied to the four components of an SG: generation, transportation, distribution, and consumption of electric energy. Therefore, the detection of anomalies is an important part of the challenges facing new smart grids.

An anomaly is a modification of the expected behavior of the system, and three types are considered: specific, context, and collective anomalies. In specific anomalies, an individual event instance may be considered anomalous compared to the rest of the dataset [5].

Context anomalies start with the notion that behavior and context are separate: the same conduct may not be regarded as an anomaly if it occurs in a different context. For example, anomalous occurrences scheduled at specific times and days of the year may not activate an anomaly detection mechanism because they are already expected [6,7].

Collective anomalies refer to instances where abnormal behavior cannot be identified by examining each event in isolation but rather by considering them as part of a collection of events [6,7].

The SG progressively plays a significant role in critical and industrial infrastructures, especially with the industry 4.0 revolution. They have become more dependent on connectivity by supporting novel communication and remote-control functionalities that expand the risks of cyber-attacks [8]. This has promoted a growing interest in studies on anomaly detection.

The physical and cybernetic infrastructures that make up an SG may present unexpected behaviors in the face of cyber-attacks, natural disasters, meteorological phenomena, events coming from the network operation itself, physical damage to network components, deviation from normal operating parameters, and overloads [9].

In this context, SGs must be able to resist anomalous events, detect them, mitigate them, and provide support for the development of a capacity to restore service or behavior quickly and safely.

2. Materials and Methods

A review of papers related to the detection of anomalies in smart grids was carried out, and bibliographic management tools and digital repositories were used to search for documents. The following stages were considered: definition of research questions, planning and definition of a search strategy, establishment of study selection criteria, identification of results, and analysis.

2.1. Definition of Research Questions

The aim of the review is to identify research studies pertaining to anomaly detection in smart electrical grids as well as analyze the trends and methodologies employed. As a result, the answers to the following questions are sought:

- What is currently known about anomaly detection?
- What are the most common AI methods?
- What is the trend in this field?

The Mendeley library management tool and electronic resources, whose search tools allow the localization of documents relevant to the review, were used: ACM Digital Library, Compendex, ScienceDirect—Elsevier, IEEE Xplore, ISI Web of Science, SpringerLink, and Wiley Inter Science Journal Finder.

In the exploration and search for manuscripts the following keywords were combined: smart grid, cyber physical systems, anomaly detection, and artificial intelligence.

2.2. Planning and Definition of the Search Strategy

The search was planned in four stages, as shown in Figure 1, beginning with automated test searches to obtain the greatest number of works that match the combination of keywords, after which they manually discarded those works that were not related to the review's objective or that were duplicates in a second stage.

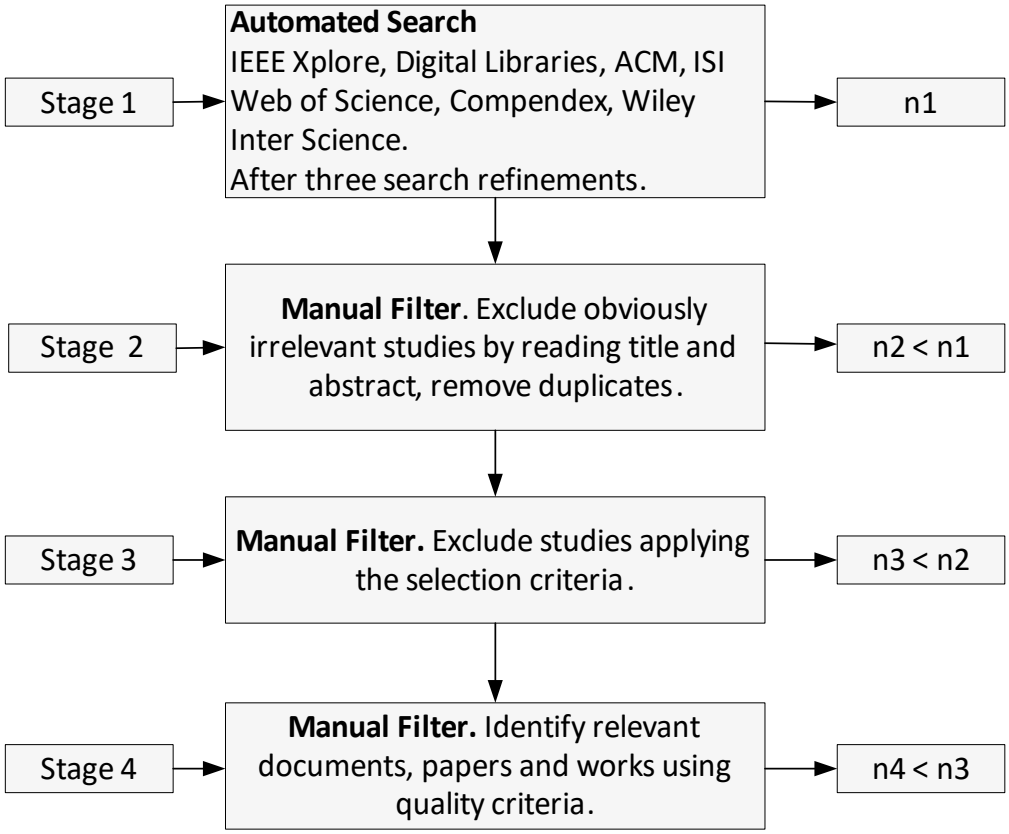

Figure 1. Stages established in the search planning. Adapted from [10].

In a third phase, the selection criteria set out in Section 2.3 are applied with the aim of reducing results and obtaining specialized manuscripts in the study area. Finally, quality criteria were applied to the results obtained in the selection phase to identify the most relevant papers.

The search approach involves utilizing automated search tools in digital repositories and bibliographic management systems to identify and organize the retrieved results and documents (Figure 2).

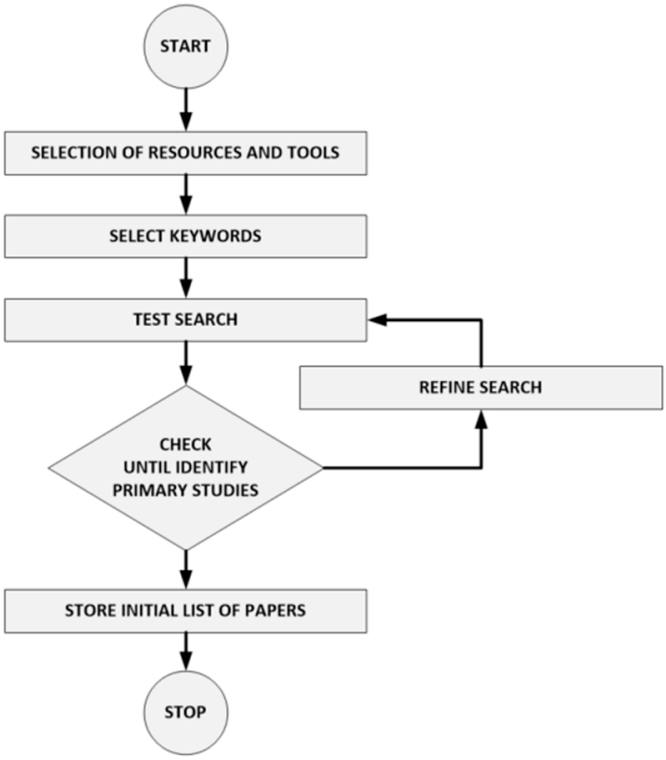

Figure 2. Flow applied in search strategy. Adapted from [11].

Test searches enable the refinement of filters to locate works pertaining to the detection methods of anomalies in SGs. Subsequently, the criteria specified during the planning stages are applied, and the resulting documents are stored for review. The search also considers the publishing date, starting from 2011 as the initial year, aligning the search with recent studies of global energy perspectives [12].

2.3. Selection and Quality Criteria

Three overarching principles are considered to determine the significance of each research project on smart grids in detecting anomalies: the work demonstrates rigor through its thorough approach and utilization of research techniques; the findings are presented in a well-structured and relevant manner, enhancing their credibility; and furthermore, the results hold relevance and practical value within the context of SGs.

The selection criteria showed in Table 1 are designed based on those three principles to discover papers that are pertinent to addressing research questions, considering their focus, aims, conclusions, findings, and study depth.

Table 1. List of selection criteria.

N.	Criteria
1	Study addresses anomaly detection in relation to smart grids
2	The study presents empirical results
3	The study presents methods and their applications
4	The study presents future lines of research

Table 2 was created to define quality criteria for selecting documents that rigorously handle the issue, are relevant, and serve as reference sources. The chosen publications were those that had consensus among two out of the three academics involved in conducting this review.

Table 2. List of quality criteria.

N.	Criteria
1	Knowledge of existing related literature is evident
2	Provides answers to research questions
3	The work enables practical applications or explores new design options
4	The solution to a real problem is being addressed
5	The work presents evidence of the validity of the findings
6	The work contrasts alternative solutions
7	The experiments are explained and reproducible

3. Results and Analysis

Table 3 lists the papers that were reviewed. The dates range from 2011 to 2023, and they provide solutions for the following: distortions in data in measurements of energy consumption, distortions in measurements of electrical signal values, network intrusions, false events in the network, anomalies that can go unnoticed, deviations in state estimates in the network, distortions in consumer prices, injection of false data, distortions in event timestamps, and device configuration changes.

The investigations rely on real or artificially created data obtained through the utilization of information and communications technology. This data is derived from network events and time series, which are saved and processed via various methods with the goal of uncovering unforeseen patterns or behaviors in the SG. In this review, seven study objects related to the detection of anomalies in SGs were identified (Table 4).

Table 3. Summary of selected documents by year. Anomaly detection.

Year	Paper
2011	[13–15]
2012	[16,17]
2013	[18]
2014	[19]
2015	[20–22]
2016	[23–27]
2017	[7,28,29]
2018	[30–35]
2019	[5,6,36–45]
2020	[8,46–56]
2021	[57–65]
2022	[66–72]
2023	[73–76]

Table 4. Grouping of issues studied for the detection of anomalies in SGs.

Study Object	Paper
Data integrity attacks	[13,21,25,29,40,41,48,49,53,55,59–62,70,75,76]
Unusual consumption behaviors and measurements	[6,24,27,32,34,35,38,46,52,67,68,71–73]
Network intrusions	[16,18,19,56,63,69]
Network infrastructure anomalies	[14,15,17,20,22,33,39,47,58,64]
Electrical data anomalies	[7,23,26,36,43–45,50,54,65,66,74]
Cyberattack detection	[8,30,37,57]
Devices for detecting anomalies	[5,28,31,42,51]

3.1. Data Integrity Attacks

These are situations in which false data injection (FDI) commonly occurs. This form of attack aims to alter the values of electrical measurements or the outcomes of a network's state estimation. The objective is to manipulate the energy price or modify the data transmitted between components of the network.

FDI can use sensors in supervisory control and data acquisition (SCADA) systems, sensors for weather monitoring, smart electricity meters, and physical communication components of neighborhood area networks (NAN) or wide area networks (WAN). Attackers usually know the network topology [40]. Technical, confidential information is in the control centers of electric utilities, and physical access is protected and regulated; therefore, it is not trivial for attackers to obtain the information, but it can happen [13]. In an FDI attack, electrical measurements such as voltage and current can be changed and even simulate a valid fault that causes switches or network protection elements to act [62].

Table 5 summarizes what will be described below. These are a series of situations on which studies have focused that aim to show applicable solutions in scenarios where an FDI occurs, such as affecting load frequency, altering the energy management system database, affecting consumption prices, phasor measurement unit data, and load forecasts. Each situation presents a different solution.

To detect an FDI relative to load frequency control, artificial neural networks (ANN) are employed because attacks of this type do not have a fixed pattern and can be nonlinear and unpredictable. A Luenberger observer is combined to estimate values and send the observed data to the ANN unit to reduce the computational load [48]. One advantage of this method is its speed and accuracy; the disadvantage compared to other methods such as machine learning or network model-based detection algorithms is that it requires at least a simple mathematical model of the system under analysis.

Table 5. Detection of data integrity attacks in SGs.

Scenario	*Method/Technique*	*Objective*
Affecting the load frequency	ANN Luenberger Observer	Identify anomalies
Attacks on EMS systems	Graphical comparisons	
FDI attacks in general	Semi-supervised learning GAN, CUSUM, CNN-LSTM, GAIN-LSTM, STDGL, Multi-tier detection schema	Detect anomalies/Mitigate attacks
Attacks on load forecasting	Supervised learning Unsupervised learning SVM, k-NN	

Anomalies involving data compromised in phasor measurement units (PMUs) can be related to load frequency control; however, from a more holistic viewpoint, the use of generative adversarial imputation networks (GAIN) combined with long short-term memory (LSTM) are also used to identify FDI with acceptable performance and computational cost [75]. This is a novel deep-learning-based data-manipulation attack resilient framework.

The combination of convolutional neural network (CNN) and LSTM proves to be useful in constructing forecast-assisted methods to identify anomalies related to FDI [70]. This model proves to be able to identify anomalies with high accuracy and low false positives, is applicable towards PMU data integrity, and shows the effectiveness of designing layered structured detection systems.

An intruder can launch an unstructured attack when they do not know the connectivity, topology, and configuration of the network, or a structured attack when they know the assets and their interconnections. In both cases, deleting or altering all or part of the database will be unusual, and the attacker will want to go unnoticed. In the face of a

stealthy attack, a graph-based approach to graph matching will help identify anomalies in the power grid database [25]. This method demonstrates a low computational load and better anomaly detection rates over principal component analysis-based and other ANN-based intrusion detection systems; the speed also stands out in this method. One limitation that can be highlighted is that the tests performed are not extensive enough to be considered the better solution; however, it is an interesting experimental alternative.

Another FDI attack is the sending of false prices to consumers. Here, the cumulative sum (CUSUM) technique is used [29], considering the control actions of the system under attack and how to design a controller that mitigates these attacks. But if there is a large variation in CUSUM samples caused by deviations in average consumption trends, more stealthy attacks could be omitted, and multi-tier detection schemes may be more effective [61]. Also, the two-tier real-time attack detection scheme compared to exponential weighted moving shows a better detection rate and fewer false alarms.

A principal issue in SG is load forecasting. There are five types of attacks: pulse, scale, ramp up or ramp down, random, and smooth curve. Here, k-means clustering is applied as an unsupervised machine learning algorithm to reconstruct the reference load data and naive Bayes classifier as the supervised machine learning algorithm for the classification of attack templates, and dynamic programming is used to calculate both the occurrence and parameter of a cyberattack on load forecast data [41]. This method is robust and has a high detection rate; however, its weakness is that it fails to find new variants of identified cyber-attacks, so improvements can be considered by incorporating multiple layers.

The possibility of affecting a wide area damping control (WADC) system by pulse attack, ramp attack, relay trigger attack, false data injection attack, or a coordinated attack combining several attacks is a real risk related to SGs. In this case, an anomaly detection algorithm with supervised machine learning and model-based logic for mitigation, support vector machine (SVM), decision trees, K-nearest neighbor (k-NN), Naive Bayes, discriminant analysis, logistic regression, and neural networks is raised as an effective option [53]. Solutions of this class that combine several methods to deal with a defined battery of specific attacks on the power grid have no clear benchmark against which to compare them; however, they can be evaluated on the accuracy of anomaly detection and in this case, the experimental result is 96.5%.

Semi-supervised learning in combination with other methods such as autoencoders and generative adversarial network (GAN), forming data-driven methods that are not dependent on specific estimation methods or system knowledge, can be effective in FDI detection and mitigation [55]. This method was evaluated against others such as semi-supervised support vector machines (S3VM), K-NN, and autoencoders, and showed a superior detection rate. This method may be ineffective against systems with variable topology; an improvement is to dynamically adapt to network changes.

Recent studies show that deep learning (DL) is valid in cybersecurity preservation applications but requires large data samples. Knowing if an FDI attack is occurring without prior samples is novel, and spatiotemporal graph deep learning (STDGL) is used for this purpose [76]. Compared to other methods, such as multi-layer perceptron (MLP), CNN, and GRU, it shows better accuracy and precision in identifying FDI attacks.

3.2. Unusual Consumption Behaviors and Measurements

Advanced metering infrastructure (AMI) is a key component because it is related to pricing, billing management, and consumption. It is targeted by cyber-attacks specializing in fraud and energy consumption patterns [24].

Non-technical losses (NTL) are economic impacts, damage to infrastructure, and decreased reliability due to fraudulent activities. In this category, there are three types of cyber-attacks known as “power overloading”:

(a) Indirect load control (ILC) cyber-attacks performed by manipulating the price curve;
(b) Direct load control mechanism (DLC) cyber-attacks, where the attacker compromises the energy management System (EMS) to send a false on or off signal;

(c) Open charge point protocol (OCPP) cyber-attacks: an attacker can damage energy security if communication channels are intercepted, and security credentials are known.

Table 6 shows a summary of the methods applied in the scenario of anomalies originating in consumption behavior or measurements.

Table 6. Methods used to identify unusual consumption behavior.

Scenario	*Method/Technique*	*Objective*
Unusual consumption behavior	DWT, VFD, ANN, DNN, DRL	Identify anomalies in HAN environment
	LP, REPTree, M5P, Random Forest, ANN, SVM	Identify anomalies in NAN + HAN environment
	Semi-supervised learning GAN	Distinguish unusual non-fraudulent consumption behavior from anomalies with fraudulent intent
	Machine Learning, K-means, LSTM, ConvLSTM, regression tree model, CNN+GRU, FL	

The smart grid can incorporate WAN, NAN, and home area networks (HAN); at the HAN level, distortion attacks can occur on energy consumption based on a threshold, knowing what the expected behavior of a consumer is. In HAN network environments, it is important to analyze energy consumption patterns. The use of DWT as well as variance fractal dimension (VFD) and ANN prove to be useful [24]. One interesting thing here is that the solution is immune to noise and considers attacks of varying duration, a few minutes or an hour, for example; the detection rate is 96% at best. An improvement is to go towards dynamic learning automation of new attack characteristics, and this could be achieved by incorporating CNN.

The IoT is increasingly present and is a key factor to consider in HAN environments. Distributed machine learning in IoT devices using a distributed neural network (DNN) is focused on smart buildings and allows for analyzing occupants' consumption behaviors as well as providing short-term energy forecasts [34]. Here, the solution aims to identify consumption behaviors for optimization and cost reduction. This is especially useful when focused on neighborhoods composed of smart buildings, where this method proves to have better results compared to SVM.

In NAN areas, there are scenarios where the fraudulent consumer reports a fraction of their energy consumed consistently; here, the use of linear programming (LP) manages to detect metering defects [32]. Other methods usually employed are SVM, decision tree, fuzzy clustering, and classification rough set theory; however, linear regression models and LP show better detection results.

Some methods cover NAN and HAN environments. These are anomaly detection frameworks based on consumption patterns, employing supervised machine learning (REPTree, M5P, Random Forest, ANN, and SVM) to detect and prevent cyber-attacks due to network overload [52]. In particular, the combination of methods called the consumption pattern-based anomaly detection framework (CPADF) shows at least experimentally a good detection rate and fewer false positives compared to other home and neighborhood network-focused solutions based on regression, neural network, and decision tree models.

Unsupervised learning is useful in scenarios where methods for detecting anomalous consumption behaviors must reduce the influence of subjective factors [35]. This method can be particularly useful in exploratory or experimental studies where little data is available, and it is suspected that there may be unusual energy consumption.

The clustering of historical time series allows for the identification of the consumption profile by K-means, and then the LSTM model, which is a particular type of RNN, serves to forecast future individual consumptions with respect to the most common profile [6].

Such solutions must consider the ability to distinguish fraudulent consumption from real changes in a customer's consumption behavior. Experiments show that models based on recurrent neural networks can be a viable alternative.

Detection of energy theft or fraudulent consumption is addressed with methods implementing a convolutional LSTM (ConvLSTM) approach that, compared to CNN-LSTM and MLP methods, can help optimize temporal data redundancy [67]. The experimental results demonstrate that ConvLSTM has strong predictive robustness, and its model structure can effectively avoid overfitting.

A recent area of study is cyber-attacks aimed at energy theft at the distributed generation level, for example, in photovoltaic panels. In this case, machine learning and regression trees are used to detect suspicious data [68]. Compared with other detectors based on SVM, autoregressive integrated moving average, and least-square error, the simulation results revealed a superior detection performance.

With respect to anomalous data that are related to the meter, the use of deep reinforcement learning (DRL) demonstrates accuracy in identification, especially in environments where thousands of metering devices are integrated into the network [71]. Compared to other methods using SVM, CNN, and LSTM, experimental results indicate that it takes less time to detect unknown attacks.

Regarding smart meters, there is a growing concern about information privacy because communications between the meter and the energy service provider's servers could be breached. Here, the federated learning (FL) anomaly detection methods were compared with centralized models. It can be noted that when the distribution of data changes between clients, FL-based methods perform worse training data than centralized models. On the other hand, FL can replace centralized models in solutions that seek to safeguard data security and privacy [73].

Hybrid models are a trend in electricity theft detection, for example, combining a gated recurrent unit (GRU) and a CNN, where the GRU extracts temporal features while the CNN retrieves abstract patterns from electrical consumption data [72]. This hybrid model has the disadvantage of a high computational cost. On the other hand, it provides better accuracy in detection compared to other hybrid models such as CNN-LSTM and MLP-LSTM.

Big Data technologies, such as Apache (Flink, Storm, Spark), Hadoop (HDFS), and KairosDB are also useful to study unusual customer consumption behaviors and discover unexpected patterns [38]. Due to the speed at which data is generated in SGs, similar solutions will be required as part of energy management systems.

3.3. Network Intrusions

Table 7 displays an overview of the findings. Sensing via sensors and supported by AI was already being studied more than a decade ago. An example being utilizing machine learning algorithms to identify and categorize abnormalities based on sensory data, which is valuable for promptly detecting unauthorized access in real time. The Decision Tree Classifier (J48) and C4.5 algorithm are used to generate a decision tree based on the provided training data [16].

The development of an intrusion detection model is subject to unknown engineering problems. It is a complex challenge and requires multiple approaches. The combination of whale optimization algorithm (WOA) as an optimization technique and ANN for classification modeling is useful in this regard [56]. The WOA can train the ANN to find the optimal weights. The model comparison results show superiority over SVM and neural networks without WOA.

Table 7. Methods related to intrusion detection in SGs.

Scenario	*Method/Technique*	*Objective*
Smart Grid Intrusions	Machine learning, Decision Tree Classifier (J48), Algorithm C4.5, Decisions Tree	Intrusion detection
	Behavioral rules specification system	Detect affected or malicious devices
	ADS host-based, ADS network-based	Detect anomalies in IED substation devices and circuit breakers
	WOA, ANN, Multi-agent architecture	Identify multiple intrusion scenarios
	PDAM	Prevent anomalies from data mining attacks

Systems based on behavioral rules seek to detect malicious devices that exploit network vulnerabilities through known or unknown attacks. These methods allow us to recognize, for example, situations in which an attacker waits for the opportunity to affect some device by taking advantage of weather conditions in which adverse operating conditions would be expected [18]. The accuracy of discriminating or recognizing intrusions and false positives means that only rule-based IDS systems today may be unsuitable for complex networks, and their combination with ML methods should be explored.

Electrical substations are susceptible to intrusions; here, host-based and network-based anomaly detection are applicable. A host-based anomaly detection system (ADS) uses logs generated by substation devices from which malicious footprints of intrusion-based steps in the substation facilities are extracted. A network-based ADS can detect malicious behaviors related to multicast messages in the substation network [19]. This kind of solution is practical but lacks mechanisms to detect unknown or undefined attacks in the algorithm, and improvement could be achieved by generating more robust hybrid methods that involve dynamic and automatic learning mechanisms.

Enhanced network user monitoring can effectively reduce the risk of data leakage, phishing, and spam attacks through the implementation of statistically based detection models and an adaptive multi-agent architecture [69]. An architecture, as such, will not indicate what a system can do, but how it should work. This is an interesting perspective, as the architecture could be implemented with different AI methods that would determine the capabilities to profile and detect intrusions.

Malicious data mining attacks can compromise sensitive user data if data packets can be intercepted through IoT network channels in SGs. The privacy-preserving data aggregation (PDAM) scheme based on the Paillier cryptosystem, and the knowledge signature mechanism shows a six-phase solution for this scenario [63]. This could be seen as a complementary proposal to detection systems, since if user data is at imminent risk, at least mechanisms would be in place to keep the data unreadable to external or internal attackers.

3.4. Network Infrastructure Anomalies

Table 8 displays an overview of the findings. Smart grid infrastructure (SGI) comprises all the tele-controlled elements, communications, sensors, hardware, and software that enable network communication and operation. Seven attack models are identified:

(a) Implants of consumption devices;
(b) Energy meter implants;
(c) Black hole attacks;
(d) Installation of malicious software;
(e) Topology attacks;
(f) Tampering with the resources of electronic devices: CPU, memory, operating systems, data, files, and configurations;

(g) Exploitation of intrinsic weaknesses in communications protocols.

Table 8. Anomaly detection in the SGI.

Scenario	*Method/Technique*	*Objective*
Network infrastructure anomalies	Construction of temporal events, Machine learning, GTP	Avoid device compromise
	Machine learning, AENN, RF	Detect time synchronization attack
	GN	Detect meter implant and network topology attacks
	SPN	Detect network topology attacks
	Pattern-based correlation capabilities, GAN	Identify anomalies in the communication protocols
	Spatiotemporal correlation, LWS, ReTAD	Detection of anomalies that are not cyber-attacks

Regarding attack models (a), (b), (c), and (d), the pattern matching scheme to detect anomalous behaviors employing graph neuron (GN) as a decentralized pattern recognition algorithm that can form an associative memory structure by interconnecting the readings from SGI devices in a graph-like structure was one of the first proposals related to this field that could be identified in this area [15]. This is currently an interesting theoretical basis that can be strengthened by considering scenarios with attackers incorporating smart stealthy mechanisms in malicious devices implanted in the SG.

In electrical substations, avoiding the compromise of intelligent electronic devices (IED) and control circuit breakers is possible through early cyber intrusion detection algorithms based on the analysis of temporal events from which four malicious characteristics can be identified: intrusion attempts; change of the file system; change of the target system configuration; and change of the target system state [14]. This is an interesting knowledge base; it provides a baseline perspective of what is being targeted in the SG infrastructure, and it is now the basis on which more automatic and intelligent methods can be structured.

Monitoring CPU usage when it exceeds a predetermined threshold that could cause services to slow down, detecting RAM overload by setting a threshold on the maximum amount of usable memory, and keeping track of the number of concurrently active tasks on a machine can all support alerting of potentially compromised devices [64]. This type of monitoring has as input a large amount of log records generated by different heterogeneous devices connected in the network and could be improved by incorporating correlation and learning mechanisms.

Temporal event analysis can be useful and has been enhanced through automation supported by agent-based supervised learning. The learning process creates signatures based on the devices considered valid or true, ground-truth profile (GTP), allowing comparison and identification of potentially compromised devices [39].

Communication protocols are subject to cyber-attacks that can cause anomalies in the SG. The use of simple network management protocol (SNMP) configured in selected devices and correlation capabilities based on detection patterns allow for the recognition of anomalies in the network [17]. We are facing the advent of new-generation smart grids as the industry must assume solutions for increasingly heterogeneous and interconnected systems. New methods adopt DNN and GAN architectures to detect operational anomalies and classify Modbus/TCP and DNP3 cyber-attacks [58]. The combination of methods in this case shows better performance than the individual models of regression, SVM, random forest, MLP, and decision tree.

Global positioning system (GPS) is an indispensable device in SGs, but it can be compromised if an attacker is able to manipulate the timestamps by spoofing a GPS signal or manipulating the precision time protocol (PTP). This is a time synchronization attack

(TSA) for which correlation analysis from historical data, unsupervised machine learning based on auto-encoder neural networks (AENN), and random forest (RF) as a supervised machine learning detector are useful [47]. The key to such solutions is the right combination of techniques in the context of attacks.

Topology attacks can be detected by using the stochastic petri net (SPN); this is a transition model that can describe system behaviors in the presence of topology attacks [33].

Not all anomalies in the SGI come from a cyber-attack; they can simply be disturbances whose origin is in the operating conditions. The spatiotemporal correlation to capture the characteristics of the anomaly inspired by the Ledoit–Wolf Shrinkage (LWS) method and real-time anomaly detection (ReTAD) algorithms allows the problem of the big volume of measurement data in anomaly detection to be overcome [20].

3.5. Electrical Data Anomalies

The treatment of problems in data collection about voltage, current, power quality, frequency, and phase angle are considered. A summary can be found in Table 9.

Table 9. Electrical data anomalies.

Scenario	*Method/Technique*	*Objective*
Voltage drops in the electrical network	SVM, Decision Tree (C4.5)	Detect anomalies
Voltage/power anomalies	Comparison of values with established ranges, Fed-SCR	
Anomalies from PMU	Unsupervised learning, HTM, MapReduce, Random matrix, isolation forest, K-Means, LoOP	
Electrical load anomalies	Hyperdimensional Computing	

Short-duration voltage sags and momentary current surges are studied using pattern recognition techniques to investigate the power signal and diagnose the voltage sag in the power grid using SVM and decision tree (DT). According to these analyses, the decision tree algorithm produces the best solution [23].

There are multiple approaches on the analysis of data coming from PMUs to detect anomalies in some of the measurements, for example: score-based detector arrays [43], hierarchical temporary memory (HTM) capable of unsupervised learning [54], application of big data tools (MapReduce) [45], random matrix theory, and new statistical models using massive data sets in the power grid [44]. In the case of HTM, a limitation is observed in not being able to classify anomalies based on the cause of the anomaly.

Machine learning is useful for the detection and classification of anomalous synchrophasor data by analyzing a selected window of data points using a combination of three unsupervised methods: isolation forest, K-means, and local outlier probability (LoOP) [65]. One interesting thing about this framework is that it does not require any training data, and experimentally, it has been observed that it can work with high accuracy in real time.

For power distribution systems, new AI techniques like hyperdimensional computing (HDC) are being used to find electrical load anomalies so that they do not have to rely on preprocessing and can focus on finding problems in real time [66]. Here, the experimental results showed better results than SVM, KNN, and LSTM, and the HDC approach works on raw data without preprocessing.

When there is not a lot of labeled data to work with, deep learning models that use federated learning and fog computing (Fed-SCR) get satisfactory results for finding power data that does not seem right [74].

3.6. Cyber-Attack Detection

There are behaviors of devices or data on the network that, compared to expected situations, can be classified as unusual, so it is important to know whether such behavior is a cyber-attack. The summary is in Table 10.

Table 10. Cyber-attack detection.

Scenario	*Method/Technique*	*Objective*
The SG is the target of diverse types of cyber-attacks.	Real-time anomaly detection framework, unsupervised machine learning, Boltzmann machine, Dynamic Bayesian Networks, PRISM, Markov chains, and decision tree.	Identify and detect anomalies

Being able to differentiate a real failure from a disturbance and a smart cyber-attack is critical. Unsupervised anomaly detection employs the Boltzmann machine to detect unobservable attacks based on free energy as the anomaly index and resorts to dynamic Bayesian networks as probabilistic graphical models that can represent the system state as a set of variables [37]. This solution was evaluated considering that occasionally an interaction between sub-systems may occur that is not necessarily an attack, that random attacks exist, or that individual or simultaneous FDI attacks may occur.

Real-time monitoring and control in SGs are critical to improving reliability and operational efficiency; therefore, in real-time anomaly detection, it is important to take advantage of AMI technology and smart meter (SM) data. This information allows real-time anomaly detection by addressing three challenges: (1) large-scale multivariate count measurements; (2) missing points; and (3) variable selection. This is intended to diagnose, classify based on control limit policies, and evaluate consumer customer facilities [30].

If an attacker uses reinforcement learning, multi-criteria analysis comes into play for all types of attacks, from network engineering to physical, software, and even social engineering. This is what not only SG managers have to worry about but, in general, all ICPS. The severity of smart attacks in industrial cyber physical systems (SSA-ICPS) framework is an example of what can be applied in this scenario considering four components: (1) the user interface to interact within the tool kernel; (2) the model builder to create and compose the model of the system and the attacker; (3) the verification engine to verify and enforce the system in case of successful attacks; and (4) the library containing templates, attack models, and countermeasures, all supported by a probabilistic symbolic model checker (PRISM), discrete-time Markov chains, continuous-time Markov chains, and Markov decision trees [8].

3.7. Devices for Detecting Anomalies

Compact and affordable devices, such as the Raspberry Pi, have proven to be useful in identifying abnormalities in an SG by analyzing data collected from PMUs. These devices can detect two types of anomalies: (1) constraint anomalies, which refer to measured values that fall outside a predetermined acceptable range determined through heuristic methods, such as voltage or current; and (2) temporal anomalies, which refer to rapid oscillations or changes in measured values within a specific time frame [28].

The use of a single board computer (SBC) in a decentralized, heterogeneous architecture to keep the computational load at acceptable levels for lower-power chipsets demonstrates that anomalies can be detected at real-time speeds [31].

Big Data technologies and techniques are present in the detection of anomalies in electricity consumption based on Big Data analytical techniques and machine learning in industrial wireless sensors (IWSN) installed in the power grid. K-NN is employed in data mining and training [51].

The anomalies can range from harmless impedance changes at some network termination to pronounced electrical faults, also considering the degradation of physical

components over time. Information about such anomalies in distribution networks can be collected using power line modems as network sensors to distinguish between localized faults, load impedance changes, and distributed faults [5].

The frequency of data collection in smart meters for early anomaly detection makes these devices increasingly relevant as specialized elements in detection [42].

4. Discussion

Research indicates that the operational components of a power management system are susceptible to many forms of abnormalities resulting from cyber-attacks, such as those affecting the topological database or device configuration, whether caused by unintentional or intentional alterations. When discussing anomalies, it is crucial to consider the harm or decay of materials and devices incorporated into the network, as well as weather conditions, and the network infrastructure.

This paper provides an initial classification of seven study objects related to SG anomalies that are amenable to AI-based methods or tools, such as distributed computing-capable devices that could give the network more intelligence. So, this classification is intended to be a contribution, and of course, it can be improved.

Each object of study describes multiple scenarios, each with different proposed solutions to detect anomalies of different natures; consequently, some solutions are not comparable. However, for each method or framework identified, we have tried to show, where possible, any weaknesses, opportunities for improvement, or alternatives against which they were evaluated.

This classification can be also a limitation of this work since it could be incomplete. We intend to improve and refine it in future works. Some papers are complex to place in one category or another as they analyze intersecting scenarios, such as unusual consumption behavior, data integrity attacks, and network intrusions.

The works reviewed address increasingly novel issues to propose optimal solutions, independent of the grid model and endowed with greater involvement of artificial intelligence, which is an evolution towards what could be called new-generation smart grids.

There are no definitive or unique anomaly detection solutions due to factors such as geographic location, installed infrastructure, and regulations. For this reason, the collection of reviewed works is a guiding reference on how to approach the study of diverse types of anomalies and can be a starting point for working to prevent anomalous behavior in SGs.

5. Conclusions

Cyber-attacks on the SGI will surely come from previous intrusions, so it is important to study how to detect a potential attack and the resulting anomalies proactively and intelligently from an intrusion.

The models proposed in the different studies reviewed give great emphasis to the use of machine learning, regression, decision trees, deep learning, support vector machines, and neural networks. Other proposals are presented in novel ways, such as federated learning, hyperdimensional computing, and graph-based methods. An increasingly visible challenge for the new models is to be able to detect anomalies by optimizing computational resources in less time, with less data, in real time, and independently of the network model.

In smart grids, experiments with synthetic data show that, compared to linear cases, nonlinear cases perform better in reducing the probability of false alarms related to anomalies.

Usually, it is about discovering malicious activities or violations of security policies through intrusion detection systems. The reviewed works show that we are evolving from signature databases to AI techniques to achieve the ability to detect new attacks starting from a referential network model, considering activities that are outside the normal model as anomalies and discriminating false positives.

There is a trend towards the formation of anomaly detection frameworks or hybrid solutions that consist of sets of various AI methods and tools combined to analyze the behavior of specific SG components.

In future work, we will go deeper into each object of study to refine it and show the evolution and trend. A further review could improve the list of study objects currently identified. In addition, the digital twins applied to SG in anomaly detection will be explored.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

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

Nomenclature

ADS	Anomaly detection system	IWSN	Industrial wireless sensors
AENN	Auto-encoder neural network	k-NN	K-nearest neighbor
AI	Artificial intelligence	LoOP	Local outlier probability
AMI	Advanced metering infrastructure	LP	Linear programming
ANN	Artificial neural networks	LSTM	Long short-term memory
CNN	Convolutional neural network	LWS	Ledoit–Wolf Shrinkage
CUSUM	Cumulative sum	NAN	Neighborhood area networks
DL	Deep learning	NTL	Non-technical losses
DLC	Direct load control mechanism	OCPP	Open charge point protocol
DNN	Distributed neural network	PMU	Phasor measurement units
DRL	Deep reinforcement learning	PTP	Precision time protocol
DT	Decision tree	ReTAD	Real-time anomaly detection
DWT	Discrete wavelet transform	RF	Random forest
FDI	False data injection	RNN	Recurrent neural networks
Fed-SCR	Federated semi-supervised class-rebalanced	SBC	Single board computer
FL	Federated learning	SG	Smart grid
GAIN	Generative adversarial imputation nets	SGI	Smart grid infrastructure
GAN	Generative adversarial network	SM	Smart meters
GN	Graph neuron	SNMP	Simple network management protocol
GPS	Global positioning system	SPN	Stochastic petri net
GRU	Gated recurrent unit	SSA-ICPS	Severity of smart attacks in industrial cyber physical systems
GTP	Ground-truth profile	STDGL	Spatiotemporal graph deep learning
HAN	Home area networks	SVM	Support vector machine
HTM	Hierarchical temporary memory	TSA	Time synchronization attack
ICPS	Industrial cyber physical systems	WADC	Wide area damping control
IED	Intelligent electronic device	WAN	Wide area networks
ILC	Indirect load control	WOA	Whale optimization algorithm

References

1. Palensky, P.; Kupzog, F. Smart Grids. *Annu. Rev. Environ. Resour.* **2013**, *38*, 201–226. [CrossRef]
2. Mocanu, E. *Machine Learning Applied to Smart Grids*; Technische Universiteit Eindhoven: Eindhoven, The Netherlands, 2017; Volume 143, p. 2017. Available online: https://research.tue.nl/en/publications/machine-learning-applied-to-smart-grids (accessed on 1 September 2023).

3. Kaitovic, I.; Lukovic, S.; Malek, M. Proactive Failure Management in Smart Grids for Improved Resilience: A Methodology for Failure Prediction and Mitigation. In Proceedings of the 2015 IEEE Globecom Workshops (GC Wkshps), San Diego, CA, USA, 6–10 December 2015; pp. 1–6. [CrossRef]
4. Chertkov, M.; Pan, F.; Stepanov, M.G. Predicting Failures in Power Grids: The Case of Static Overloads. *IEEE Trans. Smart Grid* **2011**, *2*, 162–172. [CrossRef]
5. Passerini, F.; Tonello, A.M. Smart Grid Monitoring Using Power Line Modems: Anomaly Detection and Localization. *IEEE Trans. Smart Grid* **2019**, *10*, 6178–6186. [CrossRef]
6. Fenza, G.; Gallo, M.; Loia, V. Drift-Aware Methodology for Anomaly Detection in Smart Grid. *IEEE Access* **2019**, *7*, 9645–9657. [CrossRef]
7. Rossi, B.; Chren, S.; Buhnova, B.; Pitner, T. Anomaly detection in Smart Grid data: An experience report. In Proceedings of the 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Budapest, Hungary, 9–12 October 2016; pp. 002313–002318. [CrossRef]
8. Khaled, A.; Ouchani, S.; Tari, Z.; Drira, K. Assessing the Severity of Smart Attacks in Industrial Cyber-Physical Systems. *ACM Trans. Cyber Phys. Syst.* **2021**, *5*, 10. [CrossRef]
9. De Santis, E.; Livi, L.; Mascioli, F.M.F.; Sadeghian, A.; Rizzi, A. Fault recognition in smart grids by a one-class classification approach. In Proceedings of the 2014 International Joint Conference on Neural Networks (IJCNN), Beijing, China, 6–11 July 2014; pp. 1949–1956. [CrossRef]
10. da Silva, F.Q.; Santos, A.L.; Soares, S.; França, A.C.C.; Monteiro, C.V.; Maciel, F.F. Six years of systematic literature reviews in software engineering: An updated tertiary study. *Inf. Softw. Technol.* **2011**, *53*, 899–913. [CrossRef]
11. Unterkalmsteiner, M.; Gorschek, T.; Islam, A.M.; Cheng, C.K.; Permadi, R.B.; Feldt, R. Evaluation and Measurement of Software Process Improvement—A Systematic Literature Review. *IEEE Trans. Softw. Eng.* **2012**, *38*, 398–424. [CrossRef]
12. IEA. *World Energy Outlook 2022*; IEA: Paris, France, 2022. Available online: https://www.iea.org/reports/world-energy-outlook-2022 (accessed on 1 May 2023).
13. 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*, 13. [CrossRef]
14. Ten, C.-W.; Hong, J.; Liu, C.-C. Anomaly Detection for Cybersecurity of the Substations. *IEEE Trans. Smart Grid* **2011**, *2*, 865–873. [CrossRef]
15. Baig, Z.A. On the use of pattern matching for rapid anomaly detection in smart grid infrastructures. In Proceedings of the 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm), Brussels, Belgium, 17–20 October 2011; pp. 214–219. [CrossRef]
16. Kher, S.; Nutt, V.; Dasgupta, D.; Ali, H.; Mixon, P. A detection model for anomalies in smart grid with sensor network. In Proceedings of the 2012 Future of Instrumentation International Workshop (FIIW) Proceedings, Gatlinburg, TN, USA, 8–9 October 2012; pp. 1–4. [CrossRef]
17. Subramanian, V.; Gilberti, M.; Doboli, A.; Pescaru, D. A goal-oriented programming framework for grid sensor networks with reconfigurable embedded nodes. *ACM Trans. Embed. Comput. Syst.* **2013**, *11*, 79. [CrossRef]
18. Mitchell, R.; Chen, I.-R. Behavior-Rule Based Intrusion Detection Systems for Safety Critical Smart Grid Applications. *IEEE Trans. Smart Grid* **2013**, *4*, 1254–1263. [CrossRef]
19. Hong, J.; Liu, C.-C.; Govindarasu, M. Integrated Anomaly Detection for Cyber Security of the Substations. *IEEE Trans. Smart Grid* **2014**, *5*, 1643–1653. [CrossRef]
20. Wu, J.; Xiong, J.; Shil, P.; Shi, Y. Real time anomaly detection in wide area monitoring of smart grids. In Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Jose, CA, USA, 2–6 November 2014; pp. 197–204. [CrossRef]
21. Tan, R.; Krishna, V.B.; Yau, D.K.Y.; Kalbarczyk, Z. Integrity Attacks on Real-Time Pricing in Electric Power Grids. *ACM Trans. Inf. Syst. Secur.* **2015**, *18*, 5. [CrossRef]
22. Chen, P.-Y.; Yang, S.; McCann, J.A. Distributed Real-Time Anomaly Detection in Networked Industrial Sensing Systems. *IEEE Trans. Ind. Electron.* **2015**, *62*, 3832–3842. [CrossRef]
23. Yalcin, T.; Ozdemir, M. Pattern recognition method for identifying smart grid power quality disturbance. In Proceedings of the 2016 17th International Conference on Harmonics and Quality of Power (ICHQP), Belo Horizonte, Brazil, 16–19 October 2016; pp. 903–907. [CrossRef]
24. Ghanbari, M.; Kinsner, W.; Ferens, K. Anomaly detection in a smart grid using wavelet transform, variance fractal dimension and an artificial neural network. In Proceedings of the 2016 IEEE Electrical Power and Energy Conference (EPEC), Ottawa, ON, Canada, 12–14 October 2016; pp. 1–6. [CrossRef]
25. Anwar, A.; Mahmood, A.N. Anomaly detection in electric network database of smart grid: Graph matching approach. *Electr. Power Syst. Res.* **2016**, *33*, 51–62. [CrossRef]
26. Wallace, S.; Zhao, X.; Nguyen, D.; Lu, K.-T. Chapter 17—Big Data Analytics on a Smart Grid: Mining PMU Data for Event and Anomaly Detection. In *Big Data*; Buyya, R., Calheiros, R.N., Dastjerdi, A.V., Eds.; Morgan Kaufmann: Cambridge, MA, USA, 2016; pp. 417–429. ISBN 9780128053942. [CrossRef]
27. Liu, X.; Nielsen, P.S. Regression-based Online Anomaly Detection for Smart Grid Data. *arXiv* **2016**, arXiv:1606.05781. [CrossRef]

28. Matthews, S.J.; Leger, A.S. Leveraging single board computers for anomaly detection in the smart grid. In Proceedings of the 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, NY, USA, 19–21 October 2017; pp. 437–443. [CrossRef]
29. Giraldo, J.; Cárdenas, A.; Quijano, N. Integrity Attacks on Real-Time Pricing in Smart Grids: Impact and Countermeasures. *IEEE Trans. Smart Grid* **2017**, *8*, 2249–2257. [CrossRef]
30. Moghaddass, R.; Wang, J. A Hierarchical Framework for Smart Grid Anomaly Detection Using Large-Scale Smart Meter Data. *IEEE Trans. Smart Grid* **2018**, *9*, 5820–5830. [CrossRef]
31. Drakontaidis, S.; Stanchi, M.; Glazer, G.; Hussey, J.; Leger, A.S.; Matthews, S.J. Towards Energy-Proportional Anomaly Detection in the Smart Grid. In Proceedings of the 2018 IEEE High Performance extreme Computing Conference (HPEC), Waltham, MA, USA, 25–27 September 2018; pp. 1–7. [CrossRef]
32. Yip, S.-C.; Tan, W.-N.; Tan, C.; Gan, M.-T.; Wong, K. Electrical Power and Energy Systems An anomaly detection framework for identifying energy theft and defective meters in smart grids. *Electr. Power Energy Syst.* **2018**, *101*, 189–203. [CrossRef]
33. Li, B.; Lu, R.; Choo, K.-K.R.; Wang, W.; Luo, S. On Reliability Analysis of Smart Grids under Topology Attacks: A Stochastic Petri Net Approach. *ACM Trans. Cyber-Phys. Syst.* **2018**, *3*, 10. [CrossRef]
34. Huang, H.; Xu, H.; Cai, Y.; Khalid, R.S.; Yu, H. Distributed Machine Learning on Smart-Gateway Network toward Real-Time Smart-Grid Energy Management with Behavior Cognition. *ACM Trans. Des. Autom. Electron. Syst.* **2018**, *23*, 1–26. [CrossRef]
35. Zhang, C.; Wang, F. Multi-feature Fusion Based Anomaly Electro-Data Detection in Smart Grid. In Proceedings of the 2018 15th International Symposium on Pervasive Systems, Algorithms and Networks (I-SPAN), Yichang, China, 16–18 October 2018; pp. 54–59. [CrossRef]
36. Noureen, S.S.; Bayne, S.B.; Shaffer, E.; Porschet, D.; Berman, M. Anomaly Detection in Cyber-Physical System using Logistic Regression Analysis. In Proceedings of the 2019 IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, 7–8 February 2019; pp. 1–6. [CrossRef]
37. Karimipour, H.; Geris, S.; Dehghantanha, A.; Leung, H. Intelligent Anomaly Detection for Large-scale Smart Grids. In Proceedings of the 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Edmonton, AB, Canada, 5–8 May 2019; pp. 1–4. [CrossRef]
38. Lipcàk, P.; Macak, M.; Rossi, B. Big Data Platform for Smart Grids Power Consumption Anomaly Detection. In Proceedings of the 2019 Federated Conference on Computer Science and Information Systems (FedCSIS), Leipzig, Germany, 1–4 September 2019; pp. 771–780. [CrossRef]
39. Babun, L.; Aksu, H.; Uluagac, A.S. A System-level Behavioral Detection Framework for Compromised CPS Devices: Smart-Grid Case. *ACM Trans. Cyber-Phys. Syst.* **2019**, *4*, 16. [CrossRef]
40. Yue, M.; Hong, T.; Wang, J. Descriptive Analytics Based Anomaly Detection for Cybersecure Load Forecasting. In Proceedings of the 2019 IEEE Power & Energy Society General Meeting (PESGM), Atlanta, GA, USA, 20 January 2019; p. 1. [CrossRef]
41. Cui, M.; Wang, J.; Yue, M. Machine Learning-Based Anomaly Detection for Load Forecasting Under Cyberattacks. *IEEE Trans. Smart Grid* **2019**, *10*, 5724–5734. [CrossRef]
42. Yen, S.W.; Morris, S.; Ezra, M.A.; Huat, T.J. Effect of smart meter data collection frequency in an early detection of shorter-duration voltage anomalies in smart grids. *Int. J. Electr. Power Energy Syst.* **2019**, *109*, 1–8. [CrossRef]
43. Zhou, M.; Wang, Y.; Srivastava, A.K.; Wu, Y.; Banerjee, P. Ensemble-Based Algorithm for Synchrophasor Data Anomaly Detection. *IEEE Trans. Smart Grid* **2019**, *10*, 2979–2988. [CrossRef]
44. Ling, Z.; Qiu, R.C.; He, X.; Chu, L. A New Approach of Exploiting Self-Adjoint Matrix Polynomials of Large Random Matrices for Anomaly Detection and Fault Location. *IEEE Trans. Big Data* **2021**, *7*, 548–558. [CrossRef]
45. Matthews, S.J.; Leger, A.S. Leveraging MapReduce and Synchrophasors for Real-Time Anomaly Detection in the Smart Grid. *IEEE Trans. Emerg. Top. Comput.* **2019**, *7*, 392–403. [CrossRef]
46. Tao, J.; Michailidis, G. A Statistical Framework for Detecting Electricity Theft Activities in Smart Grid Distribution Networks. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 205–216. [CrossRef]
47. Shereen, E.; Dan, G. Model-Based and Data-Driven Detectors for Time Synchronization Attacks Against PMUs. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 169–179. [CrossRef]
48. Abbaspour, A.; Sargolzaei, A.; Forouzannezhad, P.; Yen, K.K.; Sarwat, A.I. Resilient Control Design for Load Frequency Control System Under False Data Injection Attacks. *IEEE Trans. Ind. Electron.* **2020**, *67*, 7951–7962. [CrossRef]
49. Zhang, Z.; Deng, R.; Yau, D.K.Y.; Cheng, P.; Chen, J. On Hiddenness of Moving Target Defense against False Data Injection Attacks on Power Grid. *ACM Trans. Cyber-Phys. Syst.* **2020**, *4*, 25. [CrossRef]
50. Barua, A.; Muthirayan, D.; Khargonekar, P.P.; Al Faruque, M.A. Hierarchical Temporal Memory-Based One-Pass Learning for Real-Time Anomaly Detection and Simultaneous Data Prediction in Smart Grids. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 1770–1782. [CrossRef]
51. Li, M.; Zhang, K.; Liu, J.; Gong, H.; Zhang, Z. Blockchain-based anomaly detection of electricity consumption in smart grids. *Pattern Recognit. Lett.* **2020**, *138*, 476–482. [CrossRef]
52. Korba, A.A.; Tamani, N.; Ghamri-Doudane, Y.; Karabadji, N.E.I. Anomaly-based framework for detecting power overloading cyberattacks in smart grid AMI. *Comput. Secur.* **2020**, *96*, 101896. [CrossRef]
53. Ravikumar, G.; Govindarasu, M. Anomaly Detection and Mitigation for Wide-Area Damping Control using Machine Learning. *IEEE Trans. Smart Grid* **2020**, 1. [CrossRef]

54. Shi, X.; Qiu, R.; Ling, Z.; Yang, F.; Yang, H.; He, X. Spatio-Temporal Correlation Analysis of Online Monitoring Data for Anomaly Detection and Location in Distribution Networks. *IEEE Trans. Smart Grid* **2020**, *11*, 995–1006. [CrossRef]
55. 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]
56. Haghnegahdar, L.; Wang, Y. A whale optimization algorithm-trained artificial neural network for smart grid cyber intrusion detection. *Neural Comput. Appl.* **2020**, *32*, 9427–9441. [CrossRef]
57. Hasnat, A.; Rahnamay-Naeini, M. Detecting and locating cyber and physical stresses in smart grids using the k-nearest neighbour analysis of instantaneous correlation of states. *IET Smart Grid* **2021**, *4*, 307–320. [CrossRef]
58. Siniosoglou, I.; Radoglou-Grammatikis, P.; Efstathopoulos, G.; Fouliras, P.; Sarigiannidis, P. A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 1137–1151. [CrossRef]
59. Singh, V.K.; Govindarasu, M. A Cyber-Physical Anomaly Detection for Wide-Area Protection Using Machine Learning. *IEEE Trans. Smart Grid* **2021**, *12*, 3514–3526. [CrossRef]
60. Ahmed, A.; Sajan, K.S.; Srivastava, A.; Wu, Y. Anomaly Detection, Localization and Classification Using Drifting Synchrophasor Data Streams. *IEEE Trans. Smart Grid* **2021**, *12*, 3570–3580. [CrossRef]
61. Bhattacharjee, S.; Das, S.K. Detection and Forensics against Stealthy Data Falsification in Smart Metering Infrastructure. *IEEE Trans. Dependable Secur. Comput.* **2021**, *18*, 356–371. [CrossRef]
62. Qi, R.; Rasband, C.; Zheng, J.; Longoria, R. Detecting Cyber Attacks in Smart Grids Using Semi-Supervised Anomaly Detection and Deep Representation Learning. *Information* **2021**, *12*, 328. [CrossRef]
63. Wang, J.; Wu, L.; Zeadally, S.; Khan, M.K.; He, D. Privacy-preserving Data Aggregation against Malicious Data Mining Attack for IoT-enabled Smart Grid. *ACM Trans. Sen. Netw.* **2021**, *17*, 25. [CrossRef]
64. Itria, M.L.; Schiavone, E.; Nostro, N. Towards anomaly detection in smart grids by combining Complex Events Processing and SNMP objects. In Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 26–28 July 2021; pp. 212–217. [CrossRef]
65. Khaledian, E.; Pandey, S.; Kundu, P.; Srivastava, A.K. Real-Time Synchrophasor Data Anomaly Detection and Classification Using Isolation Forest, KMeans, and LoOP. *IEEE Trans. Smart Grid* **2021**, *12*, 2378–2388. [CrossRef]
66. Wang, X.; Flores, R.; Brouwer, J.; Papaefthymiou, M. Real-time detection of electrical load anomalies through hyperdimensional computing. *Energy* **2022**, *261*, 125042. [CrossRef]
67. Gao, H.-X.; Kuenzel, S.; Zhang, X.-Y. A Hybrid ConvLSTM-Based Anomaly Detection Approach for Combating Energy Theft. *IEEE Trans. Instrum. Meas.* **2022**, *71*, 2517110. [CrossRef]
68. Shaaban, M.; Tariq, U.; Ismail, M.; Almadani, N.A.; Ahmed, M. Data-Driven Detection of Electricity Theft Cyberattacks in PV Generation. *IEEE Syst. J.* **2022**, *16*, 3349–3359. [CrossRef]
69. Kisielewicz, T.; Stanek, S.; Zytniewski, M. A Multi-Agent Adaptive Architecture for Smart-Grid-Intrusion Detection and Prevention. *Energies* **2022**, *15*, 4726. [CrossRef]
70. Mahi-Al-Rashid, A.; Hossain, F.; Anwar, A.; Azam, S. False Data Injection Attack Detection in Smart Grid Using Energy Consumption Forecasting. *Energies* **2022**, *15*, 4877. [CrossRef]
71. Sun, S.; Liu, C.; Zhu, Y.; He, H.; Xiao, S.; Wen, J. Deep Reinforcement Learning for the Detection of Abnormal Data in Smart Meters. *Sensors* **2022**, *22*, 8543. [CrossRef] [PubMed]
72. Khattak, A.; Bukhsh, R.; Aslam, S.; Yafoz, A.; Alghushairy, O.; Alsini, R. A Hybrid Deep Learning-Based Model for Detection of Electricity Losses Using Big Data in Power Systems. *Sustainability* **2022**, *14*, 13627. [CrossRef]
73. Jithish, J.; Alangot, B.; Mahalingam, N.; Yeo, K.S. Distributed Anomaly Detection in Smart Grids: A Federated Learning-Based Approach. *IEEE Access* **2023**, *11*, 7157–7179. [CrossRef]
74. Abdel-Basset, M.; Moustafa, N.; Hawash, H. Privacy-Preserved Generative Network for Trustworthy Anomaly Detection in Smart Grids: A Federated Semisupervised Approach. *IEEE Trans. Ind. Inform.* **2023**, *19*, 995–1005. [CrossRef]
75. Chawla, A.; Agrawal, P.; Panigrahi, B.K.; Paul, K. Deep-learning-based data-manipulation attack resilient supervisory backup protection of transmission lines. *Neural Comput. Appl.* **2023**, *35*, 4835–4854. [CrossRef]
76. Ruan, J.; Fan, G.; Zhu, Y.; Liang, G.; Zhao, J.; Wen, F.; Dong, Z.Y. Super-Resolution Perception Assisted Spatiotemporal Graph Deep Learning Against False Data Injection Attacks in Smart Grid. *IEEE Trans. Smart Grid* **2023**, *14*, 4035–4046. [CrossRef]